SISTEM KEAMANAN DALAM MANAJEMEN E-COMMERCE

PENYUSUN

Muhammad Dominique Mendoza
Reni Rahmadani
Afandi Yusuf Lubis
Ahmad Rizal Pradana Pohan
Dezky Waldeni daulay
Dizky Waldini Daulay
Ihsan Heldi Harahap
Michael Steven F Barus
Rizky Abimayu Utama Tanjung
Romadon Nasution
Samuel Krisolit Vindonta Ginting

Editor:
Wan Safari Ramadhan

SISTEM KEAMANAN DALAM MANAJEMEN E-COMMERCE

PENULIS

Muhammad Dominique Mendoza
Reni Rahmadani
Afandi Yusuf Lubis
Ahmad Rizal Pradana Pohan
Dezky Waldeni Daulay
Dizky Waldini Daulay
Ihsan Heldi Harahap
Michael Steven F. Barus
Rizky Abimayu Utama Tanjung
Romadon Nasution
Samuel Krisolit Vindonta Ginting

EDITOR

Wan Safari Ramadhan

TANGGUH DENARA JAYA
PUBLISHER

UU No. 28 Tahun 2014 tentang Hak Cipta

Fungsi dan Sifat Hak Cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan fonogram yang telah dilakukan pengumuman sebagai bahan ajar; dan
iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000,00 (seratus juta rupiah).
2. Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

SISTEM KEAMANAN DALAM MANAJEMEN E-COMMERCE

Muhammad Dominique Mendoza
Reni Rahmadani
Afandi Yusuf Lubis
Ahmad Rizal Pradana Pohan
Dezky Waldeni Daulay
Dizky Waldini Daulay
Ihsan Heldi Harahap
Michael Steven F. Barus
Rizky Abimayu Utama Tanjung
Romadon Nasution
Samuel Krisolit Vindonta Ginting

EDITOR:
Wan Safari Ramadhan

TATA LETAK:
Wahyuni Putri Adeningsi

DESAIN SAMPUL:
Rachmadiansyah

SUMBER:
www.tdjpublisher.com

ISBN:
978-634-7193-08-7 (PDF)

UKURAN:
vii + 307 Hal; 21 cm x 29.7 cm

CETAKAN PERTAMA:
April 2025

Hak Cipta dilindungi Undang-Undang.
Dilarang menggandakan atau memperbanyak sebagian atau seluruh isi buku ini dalam bentuk apapun tanpa izin tertulis dari penerbit dan penulis.

ANGGOTA IKAPI: 006/NTT/2022
TANGGUH DENARA JAYA PUBLISHER
Jl. Timor Raya No. 130 B Oesapa Barat, Kelapa Lima
Kota Kupang, Nusa Tenggara Timur
E-mail: tdj.denarapublisher@gmail.com
Telepon: 0380-8436618/081220051382

KATA PENGANTAR

Segala puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga kami dapat menyelesaikan penyusunan buku ini dengan baik. Buku ini disusun dengan tujuan menyediakan materi pembelajaran yang relevan, sistematis, dan mudah dipahami. Kami berharap buku ini dapat menjadi referensi yang bermanfaat, khususnya bagi mahasiswa yang mempelajari bidang *E-Business*.

Kami menyadari bahwa buku ini masih memiliki kekurangan, baik dari segi isi maupun penyajiannya. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang konstruktif guna perbaikan di masa mendatang.

Semoga buku ini dapat memberikan manfaat yang luas bagi para pembaca dan berkontribusi pada dunia pendidikan.

Medan, Maret 2024

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **ii**
DAFTAR GAMBAR ..... **vi**
DAFTAR TABEL ..... **vii**
BAB 1 PENDAHULUAN **1**
1.1 Perdagangan elektronik dan *E-commerce* Keamanan 1
1.1.1 *E-commerce* dari Perspektif Keamanan 1
1.1.2 Keamanan *E-commerce* dan Pentingnya 3
1.2 Keamanan *E-commerce* Persyaratan 5
1.2.1 Keamanan *E-commerce* Elemen 5
1.3 Hirarki Logis *E-commerce* dan Persyaratan Keamanannya 7
1.3.1 Persyaratan keamanan dari berbagai lapisan logis *e-commerce* yang berbeda 7
1.4 Konten Keamanan *E-commerce* Manajemen 8
1.4.1 Konotasi Keamanan *E-commerce* Manajemen 8
1.4.2 Manajemen Keamanan *E-commerce* 11
BAB 2 Rencana Manajemen Untuk Keamanan Bisnis Online **14**
2.1 Konsep Utama 14
2.2 Elemen Rencana Manajemen Keamanan *E-Commerce* dan Jenisnya 15
2.2.1 Komponen Rencana Manajemen Keamanan *E-Commerce* 15
2.2.2 Jenis-jenis Manajemen Keamanan *E-commerce* Paket 15
2.3 Rencana Manajemen Keamanan *E-Commerce*: Persiapan dan Optimalisasi 17
2.3.1 Persiapan Rencana Manajemen Keamanan *E-Commerce* 17
2.3.2 Mengoptimalkan Rencana Manajemen Keamanan *E-Commerce* 18
2.4 Rencana Untuk Manajemen Keamanan *E-Commerce* Darurat 19
2.4.1 Gambaran Umum dari Rencana Darurat Manajemen Keamanan *E-Commerce* 19
2.4.2 Konstruksi Sistem ERP untuk Manajemen Keamanan *E-Commerce* 21
2.4.3 Konstruksi DRP untuk Manajemen Keamanan E-commerce 31
2.4.4 Konstruksi BCP untuk Manajemen Keamanan *E-Commerce* 35
BAB 3 Manajemen Keamanan *E-commerce*: Sumber Daya dan Organisasi **38**
3.1 Hubungan Sumber Daya dan Organisasi Manajemen Keamanan *E-commerce* 38
3.1.1 Definisi Sumber Daya dan Organisasi Manajemen Keamanan *E-commerce* 38
3.1.2 Hubungan Antara Sumber Daya Manajemen Keamanan E-commerce dan Organisasi 39

3.2 Sumber Daya Manajemen Keamanan E-commerce....40
3.2.1 Konfigurasi Sumber Daya Manajemen Keamanan E-Commerce....42
3.3 Organisasi Manajemen Keamanan E-commerce....47
3.3.1 Pembentukan Organisasi Manajemen Keamanan E-Commerce....48
3.3.2 Pengoperasian Organisasi Manajemen Keamanan E-commerce....54
3.3.3 Perubahan Struktur Manajemen Keamanan Perdagangan Elektronik....56
BAB 4 Mengendalikan Risiko Informasi dalam *E-commerce*....61
4.1 Proses, Peserta, dan Tanggung Jawab Manajemen Risiko Keamanan Informasi E-commerce....61
4.1.1 Proses Manajemen Risiko Keamanan Informasi....61
4.1.2 Manajemen Risiko Keamanan Informasi dan Tanggung Jawabnya....62
4.2 Penilaian dan Pengambilan Keputusan Risiko Keamanan Informasi E-commerce..63
4.2.1 Penilaian Risiko Keamanan Informasi....64
4.2.2 Keputusan Pembuangan Risiko Keamanan Informasi....72
4.3 Implementasi Pengendalian Risiko Keamanan Informasi E-commerce....73
4.3.1 Gambaran Umum Pengendalian Risiko....73
4.3.2 Tindakan Teknis....78
4.3.3 Ukuran Normatif....102
BAB 5 Mengendalikan Risiko Jaringan dalam *E-commerce*....120
5.1 Ancaman Keamanan Jaringan E-commerce dan Identifikasi Risiko....120
5.1.1 Ancaman Keamanan terhadap Jaringan E-commerce....121
5.1.2 Identifikasi Risiko Keamanan Jaringan E-commerce....125
5.2 Penilaian Risiko Keamanan Jaringan E-commerce....126
5.2.1 Elemen Penilaian Risiko Keamanan Jaringan Ecommerce....127
5.2.2 Proses Penilaian Risiko Keamanan Jaringan E-commerce....127
5.3 Implementasi Pengendalian Risiko Keamanan Jaringan Ecommerce....129
5.3.1 Model Keamanan Jaringan....130
5.3.2 Tindakan Teknis....131
5.3.3 Langkah-Langkah Regulasi....166
BAB 6 Mengendalikan Risiko Transaksi dalam *E-commerce*....178
6.1 Identifikasi Risiko Transaksi Perdagangan Elektronik....178
6.1.1 Risiko Pra-Transaksi Perdagangan Elektronik....178
6.1.2 Risiko dalam Transaksi E-commerce....182
6.1.3 Risiko Pasca-Transaksi Perdagangan Elektronik....187
6.2 Penilaian Risiko dan Pengambilan Keputusan Transaksi E-commerce....188

6.2.1 Sudut Pandang Asuransi Penilaian Risiko Transaksi E-commerce 188
6.2.2 Sistem Indeks Evaluasi Risiko Transaksi E-commerce 189
6.2.3 Keputusan Pengendalian Risiko Transaksi E-commerce 190
6.3 Implementasi Pengendalian Risiko Transaksi E-commerce 191
6.3.1 Konsep dan Properti Spesifikasi 191
6.3.2 Kepatuhan Transaksi Peserta dalam Transaksi E-commerce 194
6.3.3 Peraturan Pasar 211
6.3.4 Disiplin Diri Industri dan Pengawasan Sosial 225
BAB 7 Mengendalikan Risiko Kredit dalam *E-commerce* 228
7.1 Identifikasi Risiko Kredit E-commerce 228
7.1.1 Konsep Terkait Risiko Kredit E-commerce 228
7.1.2 Faktor Dampak dan Asal Mula Risiko Kredit E-commerce 231
7.1.3 Kinerja Risiko Kredit E-commerce 232
7.2 Penilaian dan Pengambilan Keputusan Risiko Kredit E-commerce 237
7.2.1 Gambaran Umum Evaluasi Kredit 237
7.2.2 Proses Evaluasi Risiko Kredit 245
7.2.3 Pengambilan Keputusan Pengendalian Risiko Kredit 264
7.3 Implementasi Pengendalian Risiko Kredit E-commerce 265
7.3.1 Memandu Ideologi dan Prinsip-prinsip Dasar 265
7.3.2 Mekanisme Pengendalian Risiko Kredit 266
7.3.3 Peraturan, Sistem, dan Pembangunan Integritas 272
BAB 8 Mengendalikan Risiko Personel *E-commerce* Pembangunan 274
8.1 Analisis Risiko Personel E-commerce 274
8.1.1 Perlunya Manajemen Risiko untuk Personel Ecommerce 274
8.1.2 Penyebab Risiko dan Jenis Personel E-commerce 275
8.2 Identifikasi, Penilaian, dan Pengambilan Keputusan Personel E-commerce 276
8.2.1 Identifikasi Risiko Personel E-commerce 277
8.2.2 Penilaian Risiko untuk Personel E-commerce 278
8.2.3 Keputusan Pengendalian Risiko Personel E-commerce 279
8.3 Implementasi Pengendalian Risiko untuk Personel E-commerce 281
8.3.1 Sistem Manajemen Personalia 281
8.3.2 Pendidikan dan Pelatihan Keselamatan 286
8.3.3 Meningkatkan Kesadaran Keselamatan 289
8.3.4 Pendidikan Kejujuran dan Pembangunan Budaya Integritas 291
8.3.5 Memperbaiki Mekanisme Pelatihan Personil 292

BAB 9 Sistem untuk meningkatkan Pengawasan dan Optimalisasi Manajemen Keamanan *E-commerce* 293

9.1 Sistem Pengawasan untuk Manajemen Keamanan E-Commerce 293

9.1.1 Sistem Manajemen dan Pengawasan Keamanan E-commerce yang Dinamis 293

9.1.2 Membangun Manajemen dan Pengawasan Keamanan E-commerce 298

9.2 Strategi untuk Meningkatkan Manajemen Keamanan E-Commerce 299

9.2.1 Mengoptimalkan Manajemen Keamanan E-Commerce 300

9.2.2 Pentingnya dan Tujuan Mengoptimalkan Manajemen Keamanan E-commerce yang Berkelanjutan 300

9.2.3 Implementasi Manajemen Keamanan E-Commerce 302

DAFTAR PUSTAKA 305

DAFTAR GAMBAR

Gambar 1.1 Diagram skematik sistem *e-commerce* 1
Gambar 2.1 Rencana Manajemen Keamanan E-commerce 17
Gambar 2.2 Persiapan Rencana Manajemen Keamanan *E-commerce* 18
Gambar 2.3 Konstruksi BCP untuk Manajemen Keamanan *E-Commerce* 35
Gambar 3.1 Struktur aplikasi keamanan informasi perusahaan *e-commerce* kecil dan menengah 52
Gambar 4.1 Proses spesifik manajemen risiko 61
Gambar 4.2 Isi utama dari analisis risiko 69
Gambar 4. 3 Sistem kata sandi hibrida (amplop digital) 81
Gambar 4.4 Enkripsi tautan 84
Gambar 4. 5 Enkripsi terminal 84
Gambar 4.6 Proses dasar penandatanganan tanda tangan digital 91
Gambar 4.7 Sertifikat format standar ITU-T X. 509 (versi V1) 96
Gambar 4.8 Cara melihat sertifikat digital 97
Gambar 4.9 PKI berdasarkan PEM 99
Gambar 4.10 PKI berdasarkan SET 100
Gambar 4.11 Diagram struktur infrastruktur kunci publik nirkabel 100
Gambar 5.1 Menavigasi Risiko Jaringan dalam E-commerce 120
Gambar 5.2 Ancaman dan Risiko Keamanan E-commerce 120
Gambar 5.3 Hierarki Keamanan E-commerce 121
Gambar 5.4 Penilaian Risiko Keamanan Jaringan E-commerce 126
Gambar 5.5 Memahami Penilaian Risiko Keamanan Jaringan E-commerce 127
Gambar 5.6 Mengelola Risiko Keamanan Jaringan Ecommerce 129
Gambar 5.7 Model PPDR 130
Gambar 5.8 Model PDRR 130
Gambar 5.9 Langkah-langkah Keamanan untuk E-commerce 131
Gambar 5.10 Skema Firewall Pemfilteran: Tipe dan Fungsi 135
Gambar 5.11 Skema Firewall dengan Host Ganda 135
Gambar 5.12 Skema firewall host yang memblokir 135
Gambar 5.13 Diagram skematik firewall subnet terlindung 136
Gambar 5.14 Diagram jaringan pribadi virtual 142
Gambar 5.15 Model pengendalian risiko data besar 155
Gambar 7. 1 Model dasar peringkat kredit E-commerce 241

DAFTAR TABEL

Tabel 1. 1 Analisis persyaratan keamanan konsumen.....8
Tabel 1. 2 Analisis persyaratan keamanan perusahaan.....8
Tabel 1. 3 Analisis persyaratan keamanan pemerintah.....9
Tabel 2. 1 Tingkatan darurat peristiwa keamanan informasi.....27
Tabel 4. 1 Klasifikasi aset.....65
Tabel 4. 2 Contoh penilaian.....71
Tabel 4.3 Peraturan dan dokumen normatif yang terkait dengan keamanan informasi.....116
Tabel 5.1 Nilai risiko keseluruhan dan tingkat risiko.....129
Tabel 6.1 Objek dan tanggung jawab dari spesifikasi tanggung jawab.....193
Tabel 6.2 Objek dan tanggung jawab yang berlaku dari spesifikasi panduan.....193
Tabel 7.1 Pelanggaran Kepercayaan yang Serius.....233
Tabel 7.2 Perilaku ketidakjujuran umum yang umum terjadi.....236
Tabel 7.3 Pembeli.....242
Tabel 7.4 Indeks evaluasi kredit pribadi penjual.....246
Tabel 7.5 Indeks utama evaluasi kredit ritel online untuk barang konsumsi.....249
Tabel 7.6 Indikator sekunder evaluasi kredit ritel online untuk barang konsumsi.....251
Tabel 7.7 Representasi dan deskripsi peringkat kredit Perusahaan.....263
Tabel 7.8 Presentasi dan deskripsi peringkat kredit individu.....263

BAB 1
PENDAHULUAN

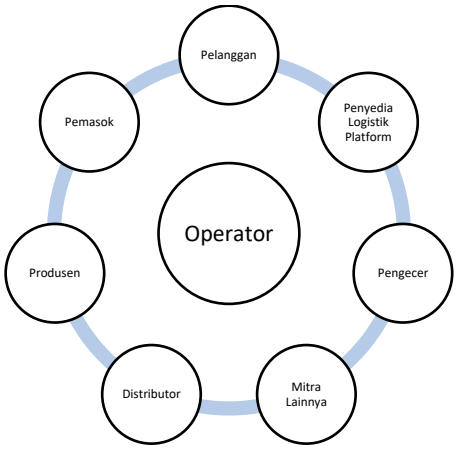
1.1 Perdagangan elektronik dan *E-commerce* Keamanan

Perdagangan elektronik mengalami transformasi dan evolusi yang sangat cepat dan keras, mulai dari awal dan kemudian menjadi saluran utama kegiatan bisnis. Menurut buku ini, *e-commerce* adalah jenis transaksi yang berbasis media jaringan informasi. Barang yang ditransaksikan dapat berupa barang material atau jasa non-material, dan proses transaksi juga dapat mencakup hak milik. Semua kegiatan bisnis yang dilakukan melalui, mengandalkan, berdasarkan, atau dengan bantuan jaringan informasi dapat dikategorikan ke dalam kategori perdagangan elektronik, karena buku ini terutama mempelajari dan membahas manajemen keamanan *e-commerce*. Dengan kata lain, semua kegiatan bisnis yang berbasis jaringan informasi elektronik diselidiki dari sudut pandang keamanan.

1.1.1 *E-commerce* dari Perspektif Keamanan

1. ***E-commerce* harus mengupayakan keamanan yang sistematis**

Pertama-tama, *e-commerce* terdiri dari operator platform, penyedia produk atau layanan, konsumen jaringan, produsen, distributor, pengecer, penyedia layanan logistik, regulator, dan kelompok lain yang terlibat dalam bisnis. Menurut teori sistem, sistem secara umum mengacu pada keseluruhan yang terdiri dari subsistem yang berbeda dalam rentang tertentu atau jenis yang sama dalam urutan dan hubungan internal tertentu. Gambar skematik sistem *e-commerce* digambarkan pada Gambar 1.1. Kedua, keamanan *e-commerce* adalah sistem. Menurut teori sistem, semua sistem memiliki karakteristik umum seperti keterbukaan, pengorganisasian diri, kompleksitas, integritas, relevansi, keseimbangan dinamis, waktu, dan sebagainya. Sistem memiliki fitur dan cara berkomunikasi dengan dunia luar.



Gambar 1.1 Diagram skematik sistem *e-commerce*

Dari perspektif teori manajemen sistem, dengan perdagangan tradisional, *e-commerce* dengan beberapa partisipasi badan utama untuk menyelesaikan, setiap subjek melalui perdagangan, efektivitas dan keamanan seluruh sistem akan sangat terpengaruh oleh keputusan yang merugikan atau berbahaya secara moral dari beberapa topik. Akibatnya, penyelidikan menyeluruh harus dilakukan pada sistem perdagangan elektronik secara keseluruhan. Teori manajemen sistem mengedepankan sistem konsep tentang struktur organisasi keseluruhan dan manajemen operasinya. Ini juga menunjukkan bahwa orang tidak hanya dapat melihat tujuan subsistem tertentu tetapi mengabaikan tujuan sistem keseluruhan. Tidak seperti perdagangan konvensional, hasil *e-commerce* dibuat oleh kerja sama berbagai organisasi. Akibatnya, buku ini menyatakan bahwa keamanan *e-commerce* harus didasarkan pada keamanan sistem secara keseluruhan sebagai tujuan utama.

2. **E-commerce pasti akan bergerak menuju tata kelola kolaboratif yang beragam**

Pertama dan terpenting, pengembangan *e-commerce* adalah proses yang membutuhkan banyak orang yang bekerja sama untuk memimpin. Teori sinergi terutama mempelajari bagaimana sebuah sistem terbuka secara spontan menghasilkan struktur yang teratur dalam waktu, ruang, dan fungsi melalui sinergi internalnya sendiri saat terjadi pertukaran materi atau energi dengan dunia luar. Berdasarkan prinsip bahwa "kerja sama banyak subsistem diatur oleh prinsip yang sama dan tidak ada hubungannya dengan karakteristik subsistem", teori sinergi memberikan ide baru bagi orang untuk memecahkan masalah yang kompleks. *E-commerce* adalah sistem yang sangat mengintegrasikan teknologi rekayasa dengan sistem ekonomi, manajemen, dan sosial. Oleh karena itu, dari perspektif keamanan, penting untuk melihat bagaimana *e-commerce* berkembang. *E-commerce* terdiri dari kolaborasi antara berbagai pihak. Subjeknya tidak hanya mencakup hal-hal yang berkaitan dengan bisnis seperti perusahaan dan konsumen, tetapi juga topik manajemen sosial seperti organisasi bisnis dan pemerintah.

Kedua, model tata kelola baru yang multi-sinergi sangat diperlukan saat *e-commerce* berkembang. Sinergisme membagi hubungan antara spesies menjadi tiga keadaan: kompetisi, predasi, dan simbiosis. Berbagai faktor biologis harus ada di setiap hubungan untuk mempertahankan pertumbuhan dan penurunan yang terkoordinasi dan keseimbangan dinamis untuk beradaptasi dan bertahan hidup di lingkungan. Selain itu, synergetics telah merancang berbagai proses kelahiran dan kematian, jaringan kelompok ekologi, dan model fenomena sosial seperti "model opini publik sosial", "model kelompok ekologi", "model meridian", "model dinamika populasi", "model sistem pemangsaan mangsa", dan "model pembentukan bentuk". Di masa mendatang, model-model ini dapat digabungkan dengan *e-commerce* yang

berbasis Konsep "struktur fungsional" adalah bagian lain dari sinergisme. Yang menyatakan bahwa struktur dan fungsi saling bergantung. Platform perdagangan elektronik, logistik, pembayaran dan penyelesaian, manufaktur, layanan, dan struktur fungsional lainnya adalah bagian dari *e-commerce*. Dengan pesatnya kemajuan teknologi informasi dan munculnya berbagai inovasi bisnis, "struktur fungsional" *e-commerce* yang tersebar tetapi tidak terpadu ini membutuhkan berbagai tata kelola yang bekerja sama untuk memastikan bahwa mereka saling bergantung, saling mempromosikan, dan berkembang bersama dengan ekonomi dan masyarakat umum.

3. **Risiko turunan yang timbul dari moda transaksi *e-commerce***

Biaya pencarian, negosiasi, dan implementasi dapat dikurangi oleh *e-commerce*, revolusi dalam transaksi bisnis konvensional. Perubahan ini, bagaimanapun, membawa masalah baru dan peluang baru. Misalnya, barang palsu, iklan palsu, penyikat pesanan, menggoreng surat, pengumpulan data pribadi yang berlebihan, dan pengungkapan data pribadi dalam transaksi online. Faktor-faktor yang memengaruhi keamanan *e-commerce* termasuk promosi, pengiriman, pengembalian uang, layanan pelanggan, logistik, dan masalah lainnya. Menurut "Laporan Pemantauan Pengalaman dan Keluhan Pengguna *E-commerce* China Q3 2020", sepuluh masalah utama yang diajukan oleh konsumen online di China pada kuartal ketiga tahun 2020 adalah sebagai berikut: masalah pengembalian dana, kualitas produk, penipuan online, masalah pengiriman, layanan purna jual, persyaratan yang berlebihan, penjualan barang palsu secara online, promosi palsu, masalah pengembalian dan penukaran, dan masalah pesanan. Terlihat bahwa masalah pengembalian dana, kualitas.

1.1.2 Keamanan *E-commerce* dan Pentingnya

1. **Definisi keamanan *e-commerce***

Menurut Standar Nasional Tiongkok (GB/T 28.001), "keamanan" adalah "keadaan di mana risiko kerusakan yang tidak dapat diterima dikecualikan." Keamanan dan risiko adalah konsep yang bertentangan satu sama lain. Objektif manajemen keamanan adalah risiko, dan tidak adanya risiko adalah ciri khas keamanan. Karena hubungan erat antara keamanan dan risiko yang disebutkan di atas, istilah "keamanan" dan "risiko" sering digunakan bersama-sama dalam buku ini. Namun, ide "risiko" yang paling penting. Dalam buku ini, definisi keamanan e-*commerce* adalah sebagai berikut: identifikasi risiko *e-commerce* dan manajemen risiko yang berkelanjutan, mengurangi risiko cedera atau kehilangan properti peserta, dan menjaga risiko dalam kisaran yang dapat diterima dari suatu negara, untuk mencapai tingkat risiko yang diharapkan dari evaluasi komprehensif operasi *e-commerce*.

Meskipun bisnis konvensional juga menghadapi masalah keamanan, masalah keamanan *e-commerce* lebih kompleks, lebih singkat, lebih luas, dan lebih mungkin berinteraksi dengan acara publik. *E-commerce* memiliki banyak topik dan banyak komponen, dan masalah keamanannya juga berasal dari topik atau komponen ini, terutama termasuk:

Keamanan informasi dan keamanan jaringan: Berbeda dengan perdagangan konvensional, setiap bisnis *e-commerce* tidak perlu melakukan aktivitas bisnis melalui jaringan. Akibatnya, pengungkapan informasi rahasia atau pribadi pengguna dengan mudah dapat menyebabkan hilangnya kepentingan semua pihak. Selain itu, keamanan jaringan dan informasi merupakan faktor penting dalam keamanan *e-commerce* karena jaringan menyediakan lingkungan operasi dasar untuk *e-commerce*.

Keamanan Transaksi: Karena transaksi adalah bagian terpenting dari *e-commerce*, keamanan transaksi harus menjadi bagian utama dari keamanan *e-commerce* karena model bisnis baru adalah tentang transaksi. Kredit dan hukum: Transaksi pasar membutuhkan kredit dan hukum. Demikian pula, *e-commerce* juga beroperasi di bawah sistem jaminan kredit tertentu dan serangkaian hukum dan peraturan. Keamanan *e-commerce* perlu memperhatikan kredit dan hukum masalah.

Keamanan personel: *E-commerce* tidak dapat berfungsi tanpa orang, jadi keamanan peserta e-commerce juga merupakan bagian penting dari keamanan *e-commerce*. Umumnya, dalam masalah keamanan di atas, keamanan *e-commerce* harus memberikan perhatian khusus pada keamanan informasi, keamanan jaringan, dan keamanan transaksi, yang merupakan masalah keamanan *e-commerce* yang paling sering terjadi di lapangan. Seperti yang ditunjukkan oleh definisi keamanan *e-commerce*, bahaya yang berkaitan dengan *e-Commerce*.

Dalam arti luas, risiko keamanan *e-commerce* mencakup semua jenis ancaman terhadap keamanan *e-commerce*, yang mencakup seluruh proses *e-commerce*, semua jenis fasilitas perangkat keras dan perangkat lunak, lingkungan operasi internal dan eksternal, termasuk risiko keamanan informasi, risiko transaksi, kredit, risiko personel, dll. Dalam arti sempit, fokus utama dari risiko keamanan *e-commerce* adalah ancaman keamanan informasi.

2. **Pentingnya keamanan e-commerce**

Pertama, keamanan *e-commerce* adalah komponen penting dari keamanan nasional Tiongkok. *E-commerce* memiliki dampak besar pada kehidupan masyarakat karena hubungannya yang erat dengan ekonomi riil, yang merupakan bagian penting dari pertumbuhan ekonomi digital Tiongkok. *E-commerce* telah melampaui perdagangan sebagai cara penting untuk alokasi sumber daya dalam kondisi informasi, dan telah menjadi kekuatan penting dalam pembangunan ekonomi dan sosial. Namun, dalam beberapa tahun terakhir, terjadi peningkatan

kejahatan seperti perusakan sistem informasi, pemalsuan atau pencurian akun, penipuan, pelanggaran rahasia *e-commerce*, pelanggaran privasi pengguna, pelanggaran hak kekayaan intelektual, dan lainnya. Keamanan *e-commerce* memengaruhi operasi biasa dan pertumbuhan *e-commerce*, serta keamanan China secara keseluruhan.

Kedua, keamanan *e-commerce* adalah komponen penting dari keamanan perusahaan karena menjamin keamanan semua pelaku *e-commerce*. Ini sangat penting bagi operator platform *e-commerce* dan penyedia produk atau layanan *e-commerce*. Karena perusahaan yang mengoperasikan platform *e-commerce* bergantung pada sistem informasi dan operasi jaringan, masalah keamanan mereka terutama terkait dengan sistem informasi dan keamanan jaringan.

E-commerce berkembang dengan cepat di era digital, dan banyak pelanggan membeli barang dasar dan layanan kehidupan melalui *e-commerce*. Oleh karena itu, keamanan *e-commerce* adalah jaminan penting bagi konsumen. Di satu sisi, keamanan *e-commerce* menjamin keamanan konsumen individu saat mereka membeli barang atau jasa melalui Internet. Keamanan konsumen terutama mencakup keamanan informasi pribadi, keamanan properti, kesehatan dan keselamatan yang disebabkan oleh kualitas produk, komunikasi yang dihasilkan, penyelesaian perselisihan, dan Proses yang mereka lakukan untuk mengonsumsi sesuatu tidak terlalu berbeda dari yang dilakukan oleh orang biasa. Namun, ketika ada masalah keamanan, akibatnya bisa lebih serius.

1.2 Keamanan *E-commerce* Persyaratan

1.2.1 Keamanan *E-commerce* Elemen

Secara umum, komponen keamanan yang diperlukan untuk keamanan *e-commerce* termasuk kerahasiaan, integritas, otentikasi, kemampuan kontrol, ketersediaan, anonimitas, kredibilitas, kepatuhan, dan legalitas. Dalam kebanyakan kasus, kerahasiaan berarti bahwa hanya pengirim dan penerima yang dapat mengakses konten informasi; orang lain tidak dapat mengakses rahasia dagang atau informasi pribadi yang terlibat dalam transaksi *e-commerce*. Untuk mengidentifikasi pelanggan, operator *e-commerce* harus meningkatkan sistem kontrol internal mereka dan prosedur manajemen teknis. Informasi pribadi termasuk nama, nomor identitas, alamat, informasi kontak, informasi lokasi, kartu bank, catatan transaksi, catatan pembayaran, dan catatan logistik.

Untuk keamanan *e-commerce*, elemen keamanan umum termasuk kerahasiaan, integritas, otentikasi, kemampuan kontrol, ketersediaan, anonimitas, kredibilitas, kepatuhan, dan legalitas. Kerahasiaan biasanya berarti bahwa hanya pengirim dan penerima yang dapat mengakses konten; orang lain tidak dapat mengakses informasi pribadi atau rahasia dagang

yang terlibat dalam transaksi *e-commerce*. Operator *e-commerce* harus meningkatkan sistem kontrol internal dan prosedur manajemen teknis untuk menemukan pelanggan. Informasi pribadi seperti nama, nomor identitas, alamat, informasi kontak, informasi lokasi, kartu bank, catatan transaksi, catatan pembayaran, dan catatan logistik termasuk dalam kategori ini.

Integritas adalah memastikan bahwa informasi dalam sistem perdagangan elektronik tidak diubah secara ilegal, rusak, hilang, dll. dengan mencegah atau memprediksi risiko, mencegah kehilangan, pengulangan, dan gangguan jahat oleh pengguna ilegal selama proses penyimpanan dan transmisi, untuk melindungi integritas informasi dan atribut terkait informasi yang dapat rusak dalam berbagai cara.

Autentikasi juga disebut keaslian, yaitu melalui mekanisme autentikasi yang dapat diandalkan untuk memastikan bahwa identitas, informasi, dan sumber informasi adalah benar. Dalam kegiatan *e-commerce*, pemalsu atau penyerang akan memalsukan identitas fisik atau informasi karena kedua belah pihak tidak dapat bertemu. Oleh karena itu, dasar dari transaksi yang aman adalah bahwa identitas atau informasi kedua belah pihak adalah nyata, yang biasanya membutuhkan intervensi pihak ketiga dan dijamin oleh mekanisme otentikasi yang dapat diandalkan. Otentikasi mencakup otentikasi entitas dan informasi. Otentikasi entitas digunakan untuk memastikan bahwa pihak-pihak yang bertransaksi adalah orang yang sebenarnya, dan otentikasi pesan dapat digunakan untuk memastikan bahwa informasi berasal dari sumber informasi yang diklaim dan bukan palsu.

P**engendalian** mengarah pada pengendalian hak akses, yang merupakan prosedur keamanan yang memastikan bahwa orang yang berwenang dapat mengakses sistem, data, dan layanan secara legal.

Non-repudiation, Juga dikenal sebagai "penyangkalan", mencegah kedua belah pihak dalam komunikasi atau transaksi untuk membantah informasi atau bisnis yang diterima. Sistem *e-commerce* harus memastikan bahwa pengirim tidak dapat membantah informasi yang dikirim dan penerima tidak dapat mengubah informasi yang diterima. Ini memastikan bahwa transaksi tidak dapat disangkal oleh kedua belah pihak dan mencegah penipuan komersial.

Ketersediaan mengarah pada jaminan bahwa sistem informasi dan informasi selalu tersedia untuk penerima hibah, bahkan dalam situasi terbatas. Ketika platform *e-commerce* besar seperti *Taobao*, *Tmall*, J*ingdong*, dll. diserang atau rusak, bahkan gangguan layanan kecil selama beberapa menit akan menyebabkan puluhan juta transaksi terpengaruh, menyebabkan pedagang atau platform mengalami kerugian yang signifikan.

Anonimitas adalah untuk melindungi hak privasi pengguna yang sah. Sistem *e-commerce* harus memastikan bahwa transaksi anonim, mencegah orang mengungkapkan informasi pribadi mereka, dan mencegah transaksi yang tidak sah dilacak.

Kredibilitas melibatkan dua aspek: kredibilitas lingkungan jaringan transaksi dan kredibilitas perilaku transaksi. Kredibilitas lingkungan jaringan memerlukan ruang verifikasi yang dapat diandalkan untuk transaksi jaringan melalui komputasi yang dapat diandalkan. Untuk memastikan bahwa perilaku transaksi dapat dipercaya, kredibilitas perilaku transaksi didasarkan pada keaslian dan keandalan identitas kedua belah pihak. Kualitas produk atau layanan, misalnya, dan apakah layanan purna jual sesuai dengan yang dijanjikan Untuk mengurangi risiko yang dibawa oleh *e-commerce* kepada kedua belah pihak, kredibilitas membutuhkan sistem evaluasi kredit karena keterbatasan teknologi dan manajemen *e-commerce*, variabel pengguna transaksi, dan ketidakpastian dan sifat transaksi *e-commerce* yang sangat dinamis.

Kepatuhan dan legitimasi mengarah pada tindakan peserta *e-commerce* yang mematuhi peraturan, hukum, dan standar nasional yang berlaku.

1.3 Hirarki Logis *E-commerce* dan Persyaratan Keamanannya

1.3.1 Persyaratan keamanan dari berbagai lapisan logis *e-commerce* yang berbeda

Sistem *e-commerce* terdiri dari tiga lapisan secara logis: lapisan jaringan, lapisan pembayaran, dan lapisan transaksi. Setiap lapisan memiliki persyaratan keamanan yang berbeda. Pada lapisan jaringan, persyaratan keamanan termasuk otentikasi, kemampuan kontrol, kerahasiaan, integritas, ketersediaan, non-repudiasi, dan kepatuhan. Pada lapisan pembayaran, persyaratan keamanan termasuk kredibilitas, kerahasiaan, integritas, ketersediaan, non-repudiasi, dan legitimasi kepatuhan.

Lapisan jaringan adalah lapisan dasar dari hirarki logis di atas. Karena permintaan yang tinggi untuk ketersediaan jaringan, lapisan jaringan harus menyediakan lingkungan jaringan yang aman dan stabil untuk perdagangan elektronik. Sangat penting bahwa data pribadi seperti nama pengguna, nomor akun, dan kata sandi disimpan di lapisan pembayaran. Lapisan transaksi sangat membutuhkan kredibilitas karena virtualitas dan ketidakpastian identitas *e-commerce*. Persyaratan keamanan dari berbagai peserta *e-commerce* Peserta utama *e-commerce* adalah pelanggan, perusahaan, dan pemerintah. Ini adalah Model *e-commerce* bisnis-ke-konsumen, atau bisnis-ke-konsumen, dapat digunakan sebagai contoh untuk menilai kebutuhan keamanan konsumen, bisnis, dan pemerintah untuk *e-commerce*.

Tabel 1. 1 Analisis persyaratan keamanan konsumen

Persyaratan keamanan	Perspektif konsumen
Kerahasiaan	Pesan saya tidak dapat dibaca oleh pihak yang tidak berwenang selain penerima yang ditunjuk
Integritas	Saya mengirim atau menerima informasi yang belum diubah atau hilang
Otentikasi	Pastikan orang atau pedagang yang saya hadapi adalah orang yang mengaku sebagai dirinya
Kemampuan kontrol	Bagaimana saya mendapatkan akses ke situs web ini, hak apa saja yang saya miliki, dan saya perlu mengontrol penggunaan informasi pribadi
Non-penolakan	Orang yang saya ajak bicara tidak dapat menyangkal bahwa transaksi telah dilakukan
Ketersediaan	Saya dapat menggunakan situs web atau platform e-commerce saat saya membutuhkannya
Anonimitas	Informasi saya tidak boleh bocor, transaksi saya tidak bisa dilacak
Kredibilitas	Tidak ada catatan konsumsi yang buruk, tidak ada evaluasi yang berbahaya
Kepatuhan dan legalitas	Perilaku konsumsi sesuai dengan hukum dan peraturan yang relevan

Tabel 1.1 dan **Tabel 1.2** menunjukkan analisis persyaratan keamanan perusahaan dan **Tabel 1.3** menunjukkan analisis persyaratan keamanan konsumen. Dari analisis di atas mengenai persyaratan keamanan dari ketiga partisipan perdagangan elektronik, dapat dilihat bahwa, karena peran mereka yang berbeda dalam perdagangan elektronik, masing-masing partisipan memiliki persyaratan keamanan yang berbeda.

1.4 Konten Keamanan *E-commerce* Manajemen

1.4.1 Konotasi Keamanan *E-commerce* Manajemen

Menggabungkan sumber daya untuk mencapai tujuan operasi keamanan *e-commerce* dikenal sebagai manajemen keamanan *e-commerce*. Tujuan utama manajemen keamanan *e-commerce* adalah untuk mengidentifikasi risiko keamanan *e-commerce* secara akurat, menilai dengan benar tingkat kerugian yang disebabkan oleh berbagai risiko keamanan *e-commerce*, menggunakan teori dan metode manajemen, dan menerapkan sarana teknis dan manajemen secara efektif dalam proses pengendalian risiko.

Tabel 1. 2 Analisis persyaratan keamanan perusahaan

Persyaratan keamanan	Perspektif bisnis
Kerahasiaan	Informasi atau data rahasia tidak dapat diakses oleh pihak yang tidak berkepentingan
Integritas	Data pada sistem informasi atau situs web tidak dibuat, dimodifikasi, atau dihapus oleh pihak yang tidak berwenang, informasi disimpan dan ditransmisikan dengan aman
Otentikasi	Memastikan identitas asli konsumen

Kemampuan kontrol	Memastikan pengoperasian normal sistem informasi atau situs web, memastikan penggunaan sumber daya dan layanan sistem oleh pengguna yang berwenang, dan mengontrol pengumpulan dan penggunaan informasi dan data pribadi konsumen dalam kisaran yang wajar
Non-penolakan	Konsumen tidak dapat menyangkal bahwa produk telah dipesan, dan rekanan tidak dapat menyangkal bahwa transaksi telah terjadi
Ketersediaan	Setiap saat dapat memberikan informasi atau layanan yang diperlukan kepada pelanggan
Anonimitas	Memastikan bahwa transaksi bersifat anonim, tidak dapat dilacak dan melindungi privasi pengguna yang sah
Kredibilitas	Meningkatkan kredibilitas lingkungan perdagangan jaringan, reputasi yang baik, tidak ada masalah kualitas barang, memberikan layanan yang konsisten dengan komitmen, tidak ada sikat tunggal
Kepatuhan dan legalitas	Produksi dan operasi sesuai dengan hukum dan peraturan nasional yang relevan, mengambil langkah-langkah efektif untuk melindungi platform atau informasi

Tabel 1. 3 Analisis persyaratan keamanan pemerintah

Persyaratan keamanan	Perspektif manajemen publik
Kerahasiaan	Pengunggahan, pembacaan, dan pengiriman informasi atau data rahasia secara legal
Integritas	Informasi disimpan dan dikirim dengan aman dan sistem transmisi tidak dirusak
Otentikasi	Memastikan identitas yang benar dan sah dari semua peserta
Kemampuan kontrol	Memastikan pengoperasian normal sistem informasi, pengumpulan dan penggunaan informasi dan data pribadi konsumen adalah legal
Non-penolakan	Pihak-pihak yang terlibat dalam transaksi tidak dapat menyangkal bahwa transaksi telah terjadi
Ketersediaan	Memastikan keamanan sistem dan memberikan informasi atau layanan yang diperlukan kepada pengguna tepat waktu
Anonimitas	Memastikan bahwa transaksi tidak dapat dilacak dan melindungi privasi secara hukum
Kredibilitas	Sistem jaringan yang digunakan untuk transaksi sesuai dengan standar perlindungan tingkat nasional yang relevan. Semua pihak yang berpartisipasi harus menghormati dan menjaga reputasi mereka sendiri dan tidak melakukan tindakan ketidakjujuran
Kepatuhan dan legalitas	Mematuhi hukum dan peraturan nasional, tidak ada niat politik yang buruk, tidak ada pelanggaran pelatihan sosial, dan adat istiadat yang baik

Selama seluruh proses *e-commerce*, manajemen keamanan memastikan pengembangan *e-commerce* yang aman dan stabil. Ini dilakukan melalui perencanaan, organisasi, sumber daya, kontrol risiko keamanan informasi, risiko keamanan jaringan, kontrol risiko keamanan transaksi, kontrol risiko kredit, kontrol risiko personil, pengawasan dan kegiatan manajemen lainnya.

Rencana: Untuk mencapai tujuan mereka, orang hari ini harus membuat berbagai macam rencana. Perencanaan adalah bagian penting dari manajemen dan harus dilakukan

sebelum tugas lainnya. Membuat tujuan manajemen keamanan *e-commerce* menjadi spesifik adalah tujuan dari rencana manajemen keamanan *e-commerce*. Untuk mencapai tujuan keamanan, manajer keamanan perdagangan elektronik membuat keputusan berdasarkan keseimbangan terus berubah dari lingkungan eksternal, kondisi internal, dan tujuan pengambilan keputusan sistem manajemen keamanan perdagangan elektronik. Untuk mencapai tujuan ini, manajer keamanan perdagangan elektronik menerapkan berbagai kegiatan kontrol dan pengaruh, sesuai dengan rencana objek manajemen keamanan perdagangan elektronik.

Sumber daya dan organisasi: Keamanan merupakan prasyarat penting bagi bisnis untuk melakukan *e-commerce*, sementara sumber daya dan organisasi merupakan jaminan penting untuk keamanan *e-commerce*. Perusahaan harus memperhatikan pembangunan sumber daya dan organisasi keamanan, terlepas dari ukuran e-commerce. Sumber daya manajemen keamanan e-commerce membantu mencapai tujuan manajemen keamanan e-commerce dan aktivitas terkait. Untuk menjamin implementasi manajemen keamanan perdagangan elektronik yang efektif, organisasi harus membuat struktur organisasi yang masuk akal, memastikan bahwa sumber daya digunakan dengan baik, dan memastikan bahwa sistem digunakan dengan benar.

Pengendalian risiko informasi dan pengendalian risiko keamanan jaringan: Berdasarkan metode manajemen risiko, keamanan informasi dan keamanan jaringan harus dikontrol, dihindari, dan dihilangkan secara efektif melalui hukum dan peraturan teknis yang relevan sehingga risiko dapat dikurangi ke tingkat yang dapat diterima. Pengendalian risiko transaksi: Risiko transaksi e-commerce dibagi menjadi risiko pra-transaksi, risiko dalam transaksi, dan risiko pasca-transaksi. Risiko pra-transaksi terutama mencakup risiko identitas, risiko iklan, dan risiko aturan perdagangan platform. Dalam hal transaksi, risiko terutama mencakup risiko penandatanganan kontrak yang ilegal, risiko gagal bayar, risiko pembayaran, dan risiko distribusi logistik, dll. Dalam hal pascatransaksi, risiko terutama mencakup risiko bukti transaksi, risiko layanan purna jual, risiko penyelesaian sengketa transaksi, dan risiko evaluasi, identitas, risiko aturan perdagangan platform, risiko distribusi logistik, evaluasi, dan risiko lainnya yang juga akan mempengaruhi aktivitas e-commerce selanjutnya.

Pengendalian risiko kredit: Kejujuran dan kepercayaan adalah standar utama perusahaan. Pada dasarnya, ekonomi pasar adalah ekonomi kredit. Jika seseorang atau organisasi ingin mendapatkan kepercayaan orang lain, mereka harus menjaga kepercayaan dan dapat mempertahankannya. Dalam e-commerce tanpa tatap muka, kredit sangat penting. Namun, aturan komersial dan sistem kredit yang tidak sempurna membahayakan pertumbuhan e-commerce yang aman.

Pengendalian risiko personel: Risiko personel dalam e-commerce mengacu pada ketidakpastian insiden keamanan dan dampak mereka terhadap organisasi. oleh tindakan karyawan e-commerce yang disengaja atau tidak disengaja. Pembangunan dan pengembangan e-commerce tidak dapat dipisahkan dari implementasi nyata dan pengoperasian personel; mereka bukan hanya komponen penting dari pembuatan dan penggunaan sistem e-commerce, tetapi juga merupakan bagian dari manajemen keamanan. Salah satu aspek penting dari manajemen keamanan perdagangan elektronik adalah risiko personel.

Mekanisme pengawasan dan optimalisasi: Keamanan adalah proses manajemen yang dinamis, dan untuk mewujudkan manajemen keamanan e-commerce, seluruh proses manajemen harus diawasi secara obyektif, penuh, dan efektif. Pada saat yang sama, untuk memastikan pertumbuhan e-commerce yang sehat dalam nilai ambang batas yang aman, perlu dibentuk mekanisme pengoptimalan tertentu.

1.4.2 Manajemen Keamanan *E-commerce*

Dalam manajemen keamanan perdagangan elektronik, ada dua komponen: sarana teknis dan sarana manajemen. Sarana teknis adalah inti dari manajemen keamanan perdagangan elektronik, dan sarana manajemen bertanggung jawab atas sarana teknis. E-commerce sering menghadapi berbagai ancaman keamanan, yang masing-masing membutuhkan satu atau lebih teknologi keamanan untuk mencegah mereka. Misalnya, teknologi otentikasi dapat mencegah serangan peniruan, teknologi kontrol akses dapat mencegah pelanggaran otorisasi, enkripsi dapat mencegah serangan eavesdropping, dan teknologi tanda tangan digital, integritas data, otentikasi, audit keamanan, pemulihan keamanan, dan teknologi lainnya dapat mencegah pelanggaran integritas. Berikut ini adalah contoh e-commerce untuk menganalisis masalah keamanan dan metode teknis yang relevan.

Keaslian mitra dagang, atau kesesuaian antara identitas asli mitra dagang dan pernyataannya Teknologi otentikasi biasanya digunakan untuk memastikan kebenaran identitas. Untuk meningkatkan keamanan, teknologi ini dapat digunakan bersama dengan infrastruktur kunci publik (PKI). Kerahasiaan dokumen elektronik dimaksudkan untuk memastikan bahwa pihak ketiga yang tidak berwenang tidak dapat mengaksesnya selama pengiriman, penyimpanan, atau pengelolaan. Enkripsi, dekripsi, dan manajemen kunci adalah teknik yang paling umum digunakan. Hilangnya dokumen elektronik, yang berarti dokumen elektronik dapat hilang selama transmisi jaringan Jika dokumen elektronik hilang, pengirim dapat menemukannya dengan memberikan nomor seri dokumen, memverifikasi nomor seri

dokumen dengan stempel waktu digital, atau melalui cara lain, seperti email, telepon, atau pesan khusus.

Integritas dokumen elektronik, yang berarti bahwa kontennya belum terkontaminasi Misalnya, jika pengguna A mengirimkan pesan "transfer 1000 yuan ke C" dan bank B menerima pesan "transfer 1000 yuan ke D", integritas pesan telah hilang. Teknologi peringkasan pesan menyelesaikan masalah ini sebagian besar.

Masalah keaslian dokumen elektronik, yang terutama diselesaikan dengan tanda tangan digital, adalah transaksi penolakan, di mana kedua belah pihak memiliki perselisihan tentang dokumen elektronik, termasuk kemungkinan pengirim atau penerima menolaknya.

Masalah ini terutama diselesaikan dengan teknologi otentikasi dan stempel waktu digital. Untuk memastikan keamanan e-commerce, teknologi keamanan tambahan diperlukan. Teknologi ini termasuk teknologi keamanan jaringan, seperti firewall, pendeteksi penyusupan, dan teknologi jaringan pribadi virtual; teknologi keamanan sistem dan aplikasi, seperti keamanan sistem operasi, basis data, keamanan Web, keamanan email, dan teknologi lainnya; dan teknologi keamanan cloud.

Alat untuk Manajemen Orang, proses, dan teknologi adalah tiga komponen utama yang mempengaruhi keamanan perdagangan elektronik. Dari ketiga komponen ini, manusia dan proses terkait dengan manajemen, sehingga dianggap sebagai tingkat manajemen. Namun, manajemen lebih penting daripada teknologi untuk mengatasi masalah keamanan.

Manajemen keselamatan e-commerce terkait erat dengan organisasi manajemen keselamatan. Organisasi ini bertanggung jawab untuk menilai ancaman keselamatan, membuat rencana dan strategi manajemen keselamatan, memantau implementasi, dan membuat peraturan keselamatan. Beberapa negara dan kelompok bisnis membuat standar keselamatan karena ada organisasi standar internasional. Organisasi Internasional untuk Standarisasi (ISO), Departemen Standarisasi Telekomunikasi Serikat Telekomunikasi Internasional (ITU-T), Federasi Pemrosesan Informasi Internasional Komite Keamanan dan Perlindungan Sistem Pemrosesan Informasi (IFIP TC11), dan Institut Insinyur Elektro dan Elektronika (IEEE). Komite Teknis Cina untuk Standardisasi Keamanan Informasi bertanggung jawab atas standarisasi pekerjaan teknis yang terkait dengan keamanan informasi karena Cina adalah anggota Organisasi Internasional untuk Standardisasi di china. Sistem manajemen perusahaan e-commerce yang relevan, standar industri yang terkait dengan keamanan e-commerce, peraturan dan kebijakan nasional, dll. adalah beberapa contoh langkah-langkah manajemen keamanan.

Karena perdagangan elektronik didasarkan pada aktivitas bisnis jaringan komputer di tingkat perusahaan, sistem manajemen keamanan informasi merupakan bagian penting dari

sistem manajemen keamanan perusahaan perdagangan elektronik. Sistem manajemen keamanan informasi menyediakan persyaratan keamanan perdagangan elektronik, yang merupakan standar dan standar manajemen keamanan perdagangan elektronik. Sistem manajemen keamanan informasi mencakup prosedur operasi, penanganan darurat, pemeliharaan harian, penyimpanan file perangkat keras dan perangkat lunak, kerahasiaan informasi, dan lainnya. Misalnya, sistem manajemen dan pemeliharaan harian sistem jaringan termasuk manajemen dan pemeliharaan harian perangkat keras dan perangkat lunak, serta sistem kesiapsiagaan virus, kerahasiaan, pelacakan dan audit, dan tindakan darurat. Sistem manajemen keselamatan perusahaan e-niaga juga mencakup sistem manajemen keselamatan untuk tahap sebelum, selama, dan setelah transaksi e-niaga, serta sistem manajemen referensi dan keselamatan personel yang sempurna.

Untuk memastikan pertumbuhan *e-commerce* yang aman dan sehat, peraturan dan perilaku peserta *e-commerce* harus dibuat. Ini memerlukan peraturan nasional dan standar industri yang berlaku. Saat ini, China secara aktif mendukung kemajuan topik ini, mengeluarkan undang-undang, standar industri, dan dasar sosial untuk mendukung pertumbuhan *e-commerce* yang aman. Keamanan *e-commerce* bergantung pada manajemen dan teknologi. Keamanan *e-commerce* hanya dapat dicapai melalui kombinasi alat administratif dan teknis.

BAB 2
Rencana Manajemen Untuk Keamanan Bisnis Online

2.1 Konsep Utama

Dalam masyarakat modern, untuk menyelesaikan tugas-tugas yang kompleks, orang perlu membuat berbagai rencana untuk memastikan kelancaran penyelesaian tugas. Perencanaan adalah suatu proses di mana suatu organisasi menentukan tujuan yang ingin dicapai dalam jangka waktu tertentu sesuai dengan kebutuhan dan karakteristiknya, dan mencapai tujuan yang diharapkan dengan mengoordinasikan berbagai sumber daya untuk perencanaan, pelaksanaan, dan pengawasan. Rencana adalah pengaturan kegiatan di masa depan. Ini adalah rencana tindakan di masa depan, mendahului kegiatan manajemen lainnya, memiliki posisi penting dalam pekerjaan manajemen organisasi.

Perencanaan memainkan peran penting dalam manajemen keselamatan. Di satu sisi, rencana manajemen keselamatan merupakan jaminan penting untuk merealisasikan tujuan keputusan keselamatan. Rencana ini menguraikan seluruh tujuan keselamatan, menghitung dan merencanakan tenaga kerja, sumber daya material, sumber daya keuangan, merumuskan langkah dan metode implementasi serta strategi dan kebijakan yang sesuai. Di sisi lain, rencana manajemen keselamatan adalah pedoman untuk pelaksanaan semua aktivitas dalam manajemen keselamatan. Untuk mencapai tujuan manajemen keselamatan, manajer keselamatan menerapkan serangkaian kegiatan pengaruh dan kontrol pada objek manajemen keselamatan sesuai dengan rencana manajemen keselamatan, dan mengoordinasikan serta memanfaatkan semua sumber daya secara wajar untuk mencapai manfaat maksimal dari kegiatan manajemen keselamatan.

Meskipun tidak semua perusahaan akan membentuk departemen manajemen keamanan khusus, tetapi manajemen keamanan tidak diragukan lagi merupakan bagian penting dari manajemen organisasi, dan begitu pula dengan perusahaan e-commerce. Karena e-commerce adalah model bisnis baru, manajemen keamanannya telah membawa tantangan baru bagi manajemen perusahaan e-commerce, jadi kita harus sangat mementingkannya. Rencana manajemen keamanan e-commerce adalah proses di mana manajer keamanan e-commerce mengkoordinasikan sumber daya terkait untuk mencapai tujuan keamanan yang diharapkan melalui persiapan, implementasi, dan pengawasan. Manajemen keamanan e-commerce dapat dilihat dari sudut pandang sempit dan luas. Keamanan e-commerce dalam arti sempit.

Perusahaan e-commerce membuat dan menerapkan rencana manajemen keselamatan selama proses pengembangan bisnis mereka. Ini disebut rencana manajemen keselamatan. Dalam arti luas, rencana manajemen keamanan e-commerce mengacu pada rencana

manajemen keselamatan yang dibuat dan diterapkan oleh perusahaan e-commerce, industri, pemerintah, dan departemen terkait. Fokus buku ini adalah rencana manajemen keamanan e-commerce dari sudut pandang sempit. Rencana darurat adalah komponen yang sangat penting dari rencana manajemen keamanan perdagangan elektronik.

2.2 Elemen Rencana Manajemen Keamanan *E-Commerce* dan Jenisnya

2.2.1 Komponen Rencana Manajemen Keamanan *E-Commerce*

Rencana manajemen keamanan perdagangan elektronik terdiri dari tiga komponen utama: tujuan manajemen keamanan perdagangan elektronik, langkah-langkah dan metode manajemen keamanan perdagangan elektronik, dan langkah-langkah.

Tujuan manajemen keamanan perdagangan elektronik: Sebelum membuat rencana manajemen keamanan perdagangan elektronik, perlu dilakukan penelitian tentang kondisi saat ini dari operasi sistem e-commerce, menilai kebutuhan manajemen keamanan e-commerce, dan mengutamakan tujuan manajemen keamanan e-commerce. Tujuan manajemen keamanan e-niaga adalah untuk mengetahui hasil pekerjaan dengan menerapkan rencana manajemen keamanan e-niaga.

Langkah-langkah dan metode manajemen keamanan perdagangan elektronik: Langkah-langkah dan metode manajemen keamanan perdagangan elektronik terutama membahas cara, keadaan, sumber daya, dan tanggung jawab untuk mencapai tujuan manajemen keamanan perdagangan elektronik yang telah ditetapkan. Mereka memastikan bahwa rencana manajemen keamanan perdagangan elektronik dapat dilaksanakan dengan lancar.

Langkah-langkah manajemen keamanan e-commerce: Langkah-langkah manajemen keamanan e-commerce membahas prosedur manajemen keamanan e-commerce dan pengaturan waktu khusus, yang mencakup total pengaturan waktu, setiap fase pengaturan waktu, deskripsi tugas, alokasi dan penggunaan sumber daya yang relevan, dan sebagainya.

2.2.2 Jenis-jenis Manajemen Keamanan *E-commerce* Paket

Rencana manajemen keamanan e-commerce dapat dibagi menjadi berbagai kategori berdasarkan standar yang berbeda. Misalnya, rencana manajemen keamanan e-commerce dapat dikategorikan berdasarkan waktu yang dihabiskan, tingkat organisasi, dan tingkat kontrol manajemen.

Rencana manajemen keamanan e-commerce dapat diklasifikasikan menjadi jangka panjang, jangka menengah, dan jangka pendek berdasarkan jangka waktu yang ditetapkan. Rencana jangka panjang biasanya terprogram dan umum dan berlangsung lebih dari 5 tahun.

Untuk menyempurnakan rencana jangka panjang, biasanya ada rencana jangka menengah dan jangka pendek. Rencana yang disebut "jangka menengah" memiliki jangka waktu sekitar lima tahun. Tidak hanya rencana jangka panjang dapat dibentuk oleh rencana ini, tetapi rencana ini juga akan memberikan dasar untuk persiapan rencana bertahap. Ini berfungsi untuk menghubungkan rencana jangka panjang dan jangka pendek, dan merupakan dasar perdagangan elektronik untuk mencapai rencana manajemen keamanan. Rencana tahunan dengan jangka waktu satu tahun biasanya disebut sebagai rencana jangka pendek. Ini adalah tanggung jawab manajemen keamanan dan tindakan tahun berjalan yang terkait yang disusun sesuai dengan rencana jangka menengah. Ini spesifik, termasuk penempatan unit pelaksana tugas dan sumber daya terkait. Ini juga mencakup rencana tindakan khusus untuk rencana jangka panjang dan jangka menengah.

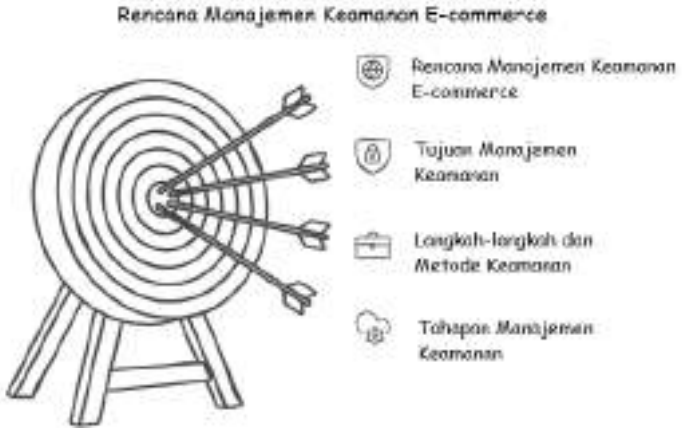
Rencana manajemen keamanan e-commerce dapat dibagi menjadi tingkat tinggi, tingkat menengah, dan akar rumput, tergantung pada tingkat organisasi. Rencana yang dibuat oleh manajemen senior dan diterapkan di seluruh perusahaan dikenal sebagai rencana tingkat tinggi. Ini adalah jenis rencana strategis yang merencanakan tugas manajemen keamanan organisasi yang signifikan dan berjangka panjang di seluruh dunia. Organisasi manajemen tingkat menengah membuat dan mengumumkan rencana tingkat menengah. Rencana tersebut juga dilaksanakan oleh akar rumput yang relevan, yang juga bertanggung jawab atas pemeriksaan rencana tersebut. Rencana tingkat menengah biasanya merupakan rencana taktis atau bisnis, yang merupakan bagian dari rencana strategis. Lembaga eksekutif akar rumput bertanggung jawab untuk menyusun dan mengeluarkan rencana akar rumput. Rencana eksekutif biasanya merupakan rencana tingkat dasar, yang biasanya mencakup rencana operasi yang aman, peraturan, dan prosedur operasi yang aman.

Rencana manajemen keamanan e-commerce dapat dibagi menjadi tingkat tinggi, tingkat menengah, dan akar rumput, tergantung pada tingkat organisasi. Rencana yang dibuat oleh manajemen senior dan diterapkan di seluruh perusahaan dikenal sebagai rencana tingkat tinggi. Ini adalah jenis rencana strategis yang merencanakan tugas manajemen keamanan organisasi yang signifikan dan berjangka panjang di seluruh dunia. Organisasi manajemen tingkat menengah membuat dan mengumumkan rencana tingkat menengah. Rencana tersebut juga dilaksanakan oleh akar rumput yang relevan, yang juga bertanggung jawab atas pemeriksaan rencana tersebut. Rencana tingkat menengah biasanya merupakan rencana taktis atau bisnis, yang merupakan bagian dari rencana strategis. Lembaga eksekutif akar rumput bertanggung jawab untuk menyusun dan mengeluarkan rencana akar rumput. Rencana

eksekutif biasanya merupakan rencana tingkat dasar, yang biasanya mencakup rencana operasi yang aman, peraturan, dan prosedur operasi yang aman.

2.3 Rencana Manajemen Keamanan *E-Commerce*: Persiapan dan Optimalisasi

Sampai batas tertentu, rencana manajemen keamanan e-commerce adalah subjektif. Oleh karena itu, prinsip, prosedur, dan metode tertentu harus diterapkan saat dibuat dan terus diubah dan ditingkatkan saat digunakan.



Gambar 2.1 Rencana Manajemen Keamanan E-commerce

2.3.1 Persiapan Rencana Manajemen Keamanan *E-Commerce*

1. **Prinsip Komunikasi**

Prinsip Ilmiah: Prinsip ilmiah mengatakan bahwa orang yang membuat rencana manajemen keamanan harus dimulai dari keadaan aktual manajemen keamanan e-commerce dan melakukan penelitian dan analisis ilmiah. Dengan demikian, rencana manajemen keamanan e-commerce harus dibuat secara ilmiah.

Prinsip Sistem: Prinsip sistematis mengacu pada bagaimana setiap bagian dari sistem objek yang direncanakan berhubungan satu sama lain, dan bagaimana hubungan antara sistem objek yang direncanakan dan sistem terkait harus dipertimbangkan saat membuat rencana manajemen keamanan e-commerce. Prinsip ini menekankan bahwa kepentingan lokal lebih penting daripada kepentingan umum untuk menjamin keamanan dan pengembangan e-commerce dalam jangka panjang, karena keduanya mempertimbangkan kebutuhan keamanan konsumen dan perusahaan e-niaga.

Prinsip praktis: Agar perusahaan e-commerce dapat mencapai tujuan manajemen yang ditetapkan melalui upaya tertentu, implementasi rencana manajemen keamanan e-commerce harus memiliki kondisi dan sumber daya yang tepat.

2. **Prosedur Persiapan**

Langkah 1: Studi dan penelitian untuk memberikan dasar untuk perencanaan rencana. Sejarah dan kondisi saat ini dari objek rencana harus diperiksa melalui penyelidikan pribadi, penyelidikan yang dipercayakan, penyelidikan kunci, penyelidikan pengambilan sampel, dan penyelidikan khusus sesuai dengan tujuan dan persyaratan rencana. Ini akan memungkinkan pemahaman menyeluruh tentang materi dan data yang relevan dan memberikan dasar untuk rencana.

Langkah Dua: Membuat ramalan keamanan Prediksi keamanan mencakup prediksi keandalan peralatan, prediksi kerentanan sistem atau perkembangan bahaya tersembunyi, prediksi kemungkinan kecelakaan, dan sebagainya. Prediksi keselamatan mencakup jangka panjang, menengah, dan jangka pendek.

Langkah 3: Membuat strategi. Tentukan tujuan manajemen keamanan e-niaga, langkah dan metode manajemen keamanan e-niaga, langkah dan instruksi terkait, dll. berdasarkan hasil penyelidikan dan prediksi keamanan. Untuk tugas yang sama yang berkaitan dengan mengelola keamanan e-commerce, beberapa opsi dapat dibuat.

Langkah 4: Memilih dan mengevaluasi rencana. Dengan menggunakan demonstrasi ilmiah, dikombinasikan dengan kondisi tertentu, manfaat dan kekurangan dari setiap rencana alternatif dievaluasi. Pada akhirnya, manajemen memilih dan menyetujui rencana terbaik.



Gambar 2.2 Persiapan Rencana Manajemen Keamanan *E-commerce*

2.3.2 Mengoptimalkan Rencana Manajemen Keamanan *E-Commerce*

Rencana manajemen keamanan e-commerce dapat diterapkan setelah dibuat. Selama implementasi rencana, rencana manajemen keamanan e-niaga harus dioptimalkan, yang berarti memeriksa dan merevisi rencana sesuai dengan situasi.

1. **Periksa Rencana Manajemen Keamanan *E-Commerce***

Pertama, pastikan bahwa rencana tersebut diterapkan dengan benar. Setiap departemen harus memastikan bahwa mereka menyelesaikan pekerjaan sesuai dengan rencana setelah implementasi rencana manajemen keamanan e-commerce.

Selanjutnya, periksa apakah rencana tersebut sesuai dengan keadaan sebenarnya. Ada kemungkinan bahwa rencana manajemen keamanan e-commerce tidak sesuai dengan pelaksanaan yang sebenarnya karena faktor-faktor seperti kesadaran publik, kondisi objektif, dan perubahan dalam lingkungan internal dan eksternal. Saat ini, kita perlu menyelidiki penyebabnya. Jika rencana itu sendiri tidak sesuai dengan keadaan sebenarnya atau jika ada masalah yang tidak terduga dalam menjalankan rencana, seperti keadaan darurat yang signifikan, rencana tersebut harus direvisi sesuai prosedur.

Selanjutnya, strategi harus dipertimbangkan. Pemantauan dilakukan sepanjang seluruh proses, dari rencana hingga implementasi. Pemantauan melibatkan pengecekan apakah pelaksanaan rencana menyimpang dari tujuan, apakah indikator rencana telah diselesaikan, apakah masalah yang muncul selama proses telah diselesaikan, apakah rencana sesuai dengan keadaan saat ini, dll.

2. **Optimalkan Rencana Manajemen Keamanan *E-Commerce***

Setelah rencana dibuat, rencana manajemen keamanan e-commerce dapat disesuaikan untuk tetap dinamis dan meningkatkan kemampuan adaptasi.

2.4 Rencana Untuk Manajemen Keamanan *E-Commerce* Darurat

2.4.1 Gambaran Umum dari Rencana Darurat Manajemen Keamanan *E-Commerce*

Dalam proses operasi, perusahaan e-dagang dapat menghadapi situasi yang mengancam keamanan mereka. Oleh karena itu, perusahaan perdagangan elektronik harus membuat rencana darurat manajemen keselamatan untuk keadaan darurat. Rencana darurat manajemen keselamatan e-commerce, juga dikenal sebagai rencana darurat manajemen keselamatan e-commerce, adalah komponen penting dari e-commerce.

Kecelakaan yang terjadi dalam bisnis e-commerce dapat disebabkan oleh banyak faktor, tetapi karena keamanan informasi sangat penting, dampak dari masalah keamanan informasi lebih besar. Oleh karena itu, buku ini membahas tentang rencana darurat manajemen keamanan e-commerce (juga dikenal sebagai "rencana darurat"), dengan fokus pada pembahasan rencana darurat keamanan informasi.

Keseluruhan proses mempersiapkan organisasi untuk menghadapi situasi yang tidak terduga dikenal sebagai perencanaan kontinjensi. Sebenarnya, perencanaan darurat adalah

prosedur kerja untuk menangani bahaya keamanan yang disebabkan oleh faktor alam dan manusia. Rencana darurat dirancang untuk memulihkan operasi perusahaan ke kondisi operasi yang dapat diterima sambil mengurangi kerugian dan gangguan. Secara umum, rencana darurat mencakup semua rencana darurat, termasuk yang berkaitan dengan hukum, transaksi, kredit, dan personalia. Rencana Tanggap Darurat (ERP), Rencana Kesinambungan Bisnis (BCP), dan Rencana Pemulihan Bencana adalah tiga komponen yang membentuk rencana darurat dalam arti sempit. Buku ini menggunakan istilah "perencanaan darurat" dalam arti sempit.

Rencana tanggap darurat, rencana keberlanjutan bisnis, dan rencana pemulihan bencana adalah bagian dari perencanaan darurat secara singkat. Rencana tanggap darurat dibuat jika peristiwa tak terduga yang disebabkan oleh faktor alam atau manusia menyebabkan kerusakan atau kerusakan nyata pada organisasi tetapi tingkat keparahannya tidak mencapai tingkat bencana. Dan ketika suatu insiden (kecelakaan) terjadi dan perusahaan e-commerce tidak dapat menghentikannya atau tidak dapat mengendalikannya, atau kecelakaan menyebabkan kerusakan yang sangat parah pada fasilitas utama sehingga perusahaan e-commerce sulit untuk pulih dengan cepat, sekarang saatnya untuk menentukan peristiwa bencana dan memulai pemulihan bencana dan rencana kesinambungan bisnis. Kelangsungan operasi dalam kasus bencana dijamin oleh rencana keberlanjutan bisnis. Rencana kesinambungan bisnis harus dimulai untuk membangun kembali operasi bisnis di tempat lain jika bencana yang parah dan berkepanjangan membuat lokasi bisnis saat ini tidak tersedia. Sementara itu, tim pemulihan bencana berkonsentrasi pada pembangunan kembali infrastruktur teknis dan pemulihan operasi bisnis. Sudah tentu, rencana keberlanjutan bisnis berbeda-beda tergantung pada organisasi dan kebutuhan bisnisnya; organisasi yang kurang berkualitas dapat menghentikan operasi hingga fasilitas utamanya diperbaiki.

Tergantung pada ukuran organisasi dan konsep bisnis, rencana tanggap darurat, kelangsungan bisnis, dan pemulihan bencana secara keseluruhan dapat digabungkan dengan ketiga rencana tersebut secara berurutan, atau rencana kelangsungan bisnis dan pemulihan bencana secara keseluruhan dapat dibuat secara terpisah. Misalnya, sebuah perusahaan besar membuat rencana tanggap darurat, kesinambungan bisnis, dan pemulihan bencana, dan membentuk tim perencanaan darurat yang sesuai. Tim ini terdiri dari perwakilan dan pemimpin koordinasi dari tim perencanaan tanggap darurat, pemulihan bencana, dan kesinambungan bisnis. Organisasi yang lebih kecil sering menggunakan tim perencanaan darurat yang lebih kecil untuk menggabungkan rencana tanggap darurat, pemulihan bencana, dan kesinambungan bisnis ke dalam satu rencana darurat.

2.4.2 Konstruksi Sistem ERP untuk Manajemen Keamanan *E-Commerce*

Perumusan rencana tanggap darurat untuk manajemen keamanan e-commerce (selanjutnya disebut rencana tanggap darurat) biasanya mencakup tiga tahap: persiapan, perencanaan, dan praktik.

1. Preparasi

Rencana tanggap darurat manajemen keamanan e-commerce biasanya terdiri dari tiga tahap: persiapan, perencanaan, dan praktik.

(1) Penilaian Potensi Risiko

Penilaian risiko adalah proses menentukan nilai aset sistem informasi, menemukan ancaman dan kerentanan sistem informasi, dan menganalisis berbagai ancaman yang mungkin terjadi. Faktor-faktor yang mengancam sistem e-commerce dapat dikategorikan menjadi faktor buatan dan faktor alami. Faktor manusia dapat dibagi menjadi faktor berbahaya dan faktor non-berbahaya berdasarkan motif ancaman yang berbeda, sedangkan faktor alam terutama mengacu pada kondisi alam yang berbahaya dan elemen fisik lainnya. Ancaman terhadap sistem informasi dapat berupa kejadian yang tidak disengaja atau disengaja atau serangan langsung atau tidak langsung yang membahayakan kerahasiaan, integritas, dan ketersediaan sistem. Sebelum mengevaluasi ancaman, kita harus mempertimbangkan apakah ancaman tersebut berasal dari faktor alam atau faktor manusia.

(2) Analisi Pengaruh Bisnis

Analisis Dampak Bisnis (BIA) adalah analisis bagaimana berbagai peristiwa keamanan informasi dapat memengaruhi operasi bisnis berdasarkan penilaian risiko, lalu menetapkan tujuan pemulihan tanggap darurat. Dalam analisis dampak bisnis, yang pertama untuk menganalisis fungsi bisnis dan situasi penggabungan sumber daya terkait, serta semua fungsi bisnis organisasi, dan menganalisis bagaimana berbagai fungsi bisnis berkorelasi satu sama lain. Untuk semua operasi bisnis, diperlukan kerahasiaan, integritas, dan ketersediaan informasi yang jelas. Kedua, sistem informasi dievaluasi untuk menentukan fungsi utama yang dilakukannya dan sumber daya yang diperlukan untuk menjalankan fungsi tersebut. Layanan atau fungsi yang jika terganggu dalam jangka waktu tertentu akan berdampak signifikan pada operasi bisnis disebut sebagai fungsi bisnis yang penting. Ketiga, dampak dari peristiwa yang berkaitan dengan keamanan data dinilai dengan menggunakan pendekatan kuantitatif atau kualitatif. Terakhir, tentukan tujuan pemulihan tanggap darurat, termasuk fungsi bisnis utama dan prioritas pemulihan. Tentukan juga rentang waktu pemulihan, yaitu rentang tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO). Target waktu pemulihan mengacu pada

berapa lama sistem informasi atau fungsi layanan harus dipulihkan setelah bencana terjadi. Saat sistem dan data harus dipulihkan setelah bencana, disebut titik pemulihan. RTO dan RPO yang sesuai untuk bisnis e-commerce dapat diidentifikasi.

(3) Konstruksi Strategi tanggap darurat

Setelah peristiwa yang mengancam keamanan data seperti gangguan layanan, kerusakan sistem, atau kerusakan jaringan terjadi, kebijakan tanggap darurat dapat digunakan untuk memulihkan sistem informasi dengan cepat dan efisien. Dalam analisis dampak bisnis, tujuan pemulihan tanggap darurat yang diidentifikasi harus menjadi bagian dari pendekatan ini.

Pertama, tentukan kapasitas pemulihan sistem. Kemampuan sistem dibagi menjadi enam tingkat: dukungan dasar; dukungan situs cadangan; transmisi elektronik dan dukungan peralatan parsial; transmisi elektronik dan dukungan peralatan lengkap; transmisi data waktu nyata dan dukungan peralatan lengkap; kehilangan data nol; dan dukungan klaster jarak jauh.

Kedua, kebutuhan akan sumber daya untuk pemulihan sistem. Persyaratan berikut berlaku untuk masing-masing kategori sumber daya.

Sistem pencadangan data terdiri dari media pencadangan data, perangkat lunak, dan perangkat keras. Sistem pencadangan data yang bergantung pada transmisi elektronik juga memiliki jalur pencadangan data dan peralatan komunikasi yang tepat. Untuk perusahaan e-commerce, sistem pencadangan data dapat dibuat oleh organisasi itu sendiri atau disewa dari organisasi lain.

Semua peralatan pemrosesan data yang diperlukan untuk pemulihan sistem disebut sebagai sistem pemrosesan data cadangan. Untuk mendapatkan sistem pemrosesan data siaga, Anda harus terlebih dahulu menandatangani perjanjian pasokan darurat dengan produsen; membeli peralatan pemrosesan data yang diperlukan dan menyimpannya di pusat pencadangan bencana (yang akan menggantikan sistem pemrosesan data utama dan mendukung operasi bisnis utama setelah bencana) atau di gudang peralatan yang aman.

Pengguna akhir menggunakan jaringan yang dimaksudkan untuk mendukung sistem pemrosesan data siaga; ini termasuk peralatan komunikasi jaringan siaga dan jalur komunikasi data siaga. Seperti sistem pemrosesan data siaga, peralatan komunikasi jaringan siaga juga diperoleh. Untuk mendapatkan jalur komunikasi data siaga, Anda dapat menggunakan jalur komunikasi data pribadi Anda atau menyewa jalur komunikasi data publik.

Infrastruktur siaga mencakup semua struktur, peralatan, dan organisasi yang diperlukan untuk pemulihan sistem dan mendukung pengoperasian sistem pencadangan. Ini termasuk tempat penyimpanan di luar lokasi untuk media pencadangan data, ruang untuk peralatan pencadangan, fasilitas tambahan untuk pemulihan sistem, dan fasilitas tempat tinggal yang

memungkinkan personel pemulihan sistem tinggal secara terus menerus. Salah satu cara untuk mendapatkan infrastruktur siaga adalah sebagai berikut: organisasi memiliki atau menjalankan infrastruktur siaga; beberapa pihak memiliki akses ke infrastruktur siaga melalui perjanjian timbal balik atau melalui penyewaan; atau pusat cadangan komersial.

Kemampuan dukungan teknis: Kemampuan untuk memberikan dukungan dan jaminan lengkap untuk pengoperasian sistem pemulihan untuk mencapai tujuan yang diharapkan. pemulihan sistem mencakup kemampuan untuk mengelola operasi dan komunikasi sistem jaringan yang aman serta pemecahan masalah perangkat keras, perangkat lunak sistem, dan perangkat lunak aplikasi. Anda dapat memperoleh kemampuan dukungan teknis melalui: staf dukungan teknis penuh waktu di pusat cadangan; kontrak dukungan teknis atau layanan dengan produsen; atau staf teknis dari pusat utama yang bekerja paruh waktu, tetapi perlu diperhatikan bahwa staf dukungan teknis tidak dapat membantu saat insiden keamanan informasi terjadi.

Operasi dan manajemen: Manajemen operasi dan pemeliharaan mencakup manajemen lingkungan operasi, manajemen sistem, manajemen keamanan, manajemen perubahan, dan sebagainya. Mempercayakan operasi dan pemeliharaan kepada perusahaan lain berarti mengakuisisi kemampuan operasi dan manajemen.

Rencana pemulihan sistem: file yang menjelaskan tugas, tindakan, data, dan sumber daya yang diperlukan selama pemulihan sistem. Ini membantu personel terkait memulihkan fungsi layanan utama yang didukung sistem untuk mencapai tujuan pemulihan sistem yang telah ditetapkan. Perusahaan e-commerce dapat mendapatkan rencana pemulihan sistem dengan menyelesaikannya secara mandiri; mempekerjakan ahli eksternal untuk membantunya menyelesaikannya; atau mempercayakannya kepada organisasi eksternal.

Terakhir, pikirkan tentang biaya. Perusahaan e-commerce harus memastikan bahwa mereka memiliki staf dan dana yang cukup untuk menerapkan strategi tanggap darurat yang dipilih. Anggaran harus memungkinkan pengeluaran untuk penggantian peralatan, lokasi cadangan yang berbeda, dan biaya lainnya. Perangkat keras, perangkat lunak, pengujian, pelatihan, tenaga kerja, layanan kontrak, dan perjalanan dan transportasi harus menjadi bagian dari anggaran. Perusahaan e-commerce harus melakukan analisis biaya-manfaat untuk membuat rencana tanggap darurat terbaik.

2. Perencanaan

Selama insiden keamanan informasi, rencana tanggap darurat harus menyediakan panduan yang cepat dan jelas bagi individu atau sistem yang belum terbiasa dengan rencana tersebut. Rencana tanggap darurat harus jelas, ringkas, dan mudah diterapkan, dengan daftar periksa dan prosedur jika memungkinkan. Dokumen rencana tanggap darurat terdiri dari enam bagian:

aturan umum, peran dan tanggung jawab, mekanisme pencegahan dan peringatan dini, proses tanggap darurat, langkah-langkah perlindungan tanggap darurat, dan lampiran.

(1) Aturan Umum

Ketentuan umum membuat rencana tanggap darurat lebih mudah dipahami, dilaksanakan, dan dipelihara dengan memberikan latar belakang atau informasi yang relevan. Tujuan penyusunan, dasar penyusunan, ruang lingkup penerapan, prinsip kerja, dll. biasanya dimasukkan dalam ketentuan umum.

(2) Peran dan Tanggung Jawab

(3) Metode Pencegahan

Perusahaan e-commerce harus membuat tim tanggap darurat keamanan informasi berdasarkan operasi hariannya dan menentukan siapa yang bertanggung jawab. Personel manajemen, operasional, teknis, dan logistik administratif membentuk organisasi tanggap darurat. Orang-orang ini terbagi menjadi lima kelompok fungsional berdasarkan tugas mereka: pemimpin tanggap darurat, dukungan teknis tanggap darurat, ahli tanggap darurat, implementasi tanggap darurat, dan kelompok operasional harian tanggap darurat, seperti yang ditunjukkan pada Gambar 2.1 Perlu diingat bahwa rencana tanggap darurat harus dilaksanakan di bawah komando terpadu dari kelompok pimpinan tanggap darurat, yang harus terdiri dari anggota manajemen puncak organisasi. Kelompok pimpinan tanggap darurat terutama bertanggung jawab untuk mendukung pekerjaan tanggap darurat, termasuk menerbitkan dokumen resmi dan menyediakan sumber daya yang diperlukan; meninjau dan menyetujui strategi tanggap darurat; meninjau dan menyetujui rencana tanggap darurat; menyetujui dan mengawasi pelaksanaan rencana tanggap darurat; dan bertanggung jawab atas koordinasi internal dan eksternal organisasi.

Di sisi lain, informasi harus dipantau dan dikomunikasikan oleh organisasi. Selain itu, sistem untuk pelaporan dan pemberitahuan insiden keamanan data juga harus dibuat selain meningkatkan pemantauan, analisis, dan peringatan dini yang berkaitan dengan keamanan data. Setelah terjadi masalah keamanan informasi, unit atau departemen harus segera melaporkannya kepada tim operasi harian tanggap darurat. Tim operasi harian tanggap darurat harus melakukan verifikasi awal setelah menerima laporan insiden keamanan informasi; kemudian, mereka harus segera melaporkannya kepada tim pimpinan tanggap darurat, mensintesis keadaan, mengevaluasi potensi kerusakan, dan membuat rencana tindakan awal. Untuk membuat rencana aksi dan mengeluarkan, tim pimpinan tanggap darurat mengadakan rapat koordinasi.

Instruksi dan instruksi. Sebaliknya, organisasi harus secara aktif menerapkan sistem perlindungan keamanan informasi. Saat membangun jaringan dan sistem informasi dasar, mereka harus sepenuhnya mempertimbangkan mekanisme pemulihan bencana dan ketahanan kerusakan. Perusahaan e-commerce harus melatih personel terkait dalam mekanisme pencegahan dan peringatan dini, sehingga mereka tahu bagaimana dan kapan menggunakannya. Mekanisme pencegahan dan peringatan dini harus dijaga dalam kondisi baik untuk memastikan bahwa mereka berfungsi dengan baik dalam insiden keamanan informasi.

(4) Metode Tanggap Darurat

Proses tanggap darurat mencakup rangkaian tindakan yang diperlukan untuk menangani situasi darurat secara wajar dan efektif setelah peristiwa yang mengancam keamanan data. Proses tanggap darurat terdiri dari lima bagian: pemberitahuan kejadian keamanan informasi, klasifikasi dan penilaian kejadian, pembentukan rencana tanggap darurat, penanganan keadaan darurat, dan pasca-pemrosesan.

Pemberitahuan yang berkaitan dengan masalah keamanan data Informasi pemberitahuan, laporan informasi, dan pengungkapan informasi adalah tiga komponen dari peringatan peristiwa keamanan informasi. Komunikasi terjadi secara "horizontal". Dalam organisasi, pemberitahuan informasi berarti bahwa unit atau departemen yang mengalami insiden keamanan informasi harus memberi tahu tim operasi harian tanggap darurat. Tim ini akan menilai tingkat kerusakan dan memutuskan apa yang harus dilakukan selanjutnya. Tim Operasi Harian Tanggap Darurat harus menginformasikan Tim Pimpinan Tanggap Darurat setelah evaluasi kerusakan selesai. Pemberitahuan informasi adalah inti dan kunci dalam menangani insiden keamanan informasi; ini menentukan seberapa cepat dan efektif perusahaan e-commerce menangani insiden ini. Di luar pelaporan insiden keamanan informasi, unit atau departemen harus segera memberi tahu pihak yang terkena dampak organisasi eksternal yang berbahaya, unit terkait, dan pengguna penting. Jika ada kebutuhan tanggap darurat, juga harus secara akurat melaporkan informasi tersebut ke peralatan, fasilitas, dan penyedia layanan yang relevan untuk mendapatkan dukungan tangga. Pemberitahuan "vertikal" disebut pelaporan informasi. Setelah terjadi masalah keamanan informasi, unit atau departemen yang bertanggung jawab harus segera mencatat situasi atau melaporkannya kepada supervisor atau unit/departemen pengawas yang relevan sesuai dengan peraturan dan persyaratan. Secara umum, insiden keamanan informasi tingkat rendah harus dilaporkan, sedangkan insiden tingkat tinggi dapat diarsipkan dan diserahkan kepada pengawas atasan atau departemen pengawas dalam bentuk laporan bulanan, triwulanan, atau tahunan untuk penelitian pelacakan dan prediksi situasi keamanan jangka panjang. Menurut tingkat keparahan insiden keamanan

informasi, pengungkapan informasi adalah organisasi yang menunjuk kelompok tertentu untuk memberikan informasi yang relevan kepada media secara tepat waktu untuk mencegah spekulasi dan perpecahan pendapat publik.

Penyebutan dan evaluasi peristiwa Tim operasi harian tanggap darurat mengevaluasi dan mengkategorikan insiden keamanan informasi setelah terjadi masalah keamanan informasi. Penilaian kerusakan berkonsentrasi pada analisis sistem bisnis atau wilayah yang terkena dampak, potensi dampak atau kerugian tambahan (seperti bencana sekunder), faktor logistik, status total dan fungsional peralatan sistem, jenis peralatan sistem yang hilang, item yang harus diganti, dan waktu yang diperlukan untuk memulihkan layanan normal. Setelah penilaian kerusakan selesai, jenis kejadian yang mengancam keamanan data harus ditentukan.

Ada kemungkinan bahwa masalah keamanan informasi terjadi karena kelalaian, kesalahan, atau faktor non-manusia. Dalam hal keamanan informasi, peristiwa dapat dikategorikan menjadi tujuh kategori utama: peristiwa program berbahaya, serangan jaringan, perusakan informasi, peristiwa keamanan konten informasi, kegagalan peralatan dan fasilitas, bencana, dan peristiwa keamanan informasi lainnya. Kejadian program berbahaya terjadi ketika program berbahaya dibuat dan disebarkan dengan tidak sengaja atau terpengaruh olehnya. Program berbahaya akan mengganggu data sistem, aplikasi, kerahasiaan, integritas, ketersediaan, atau operasi normal sistem informasi. Peristiwa serangan jaringan mengacu pada peristiwa keamanan informasi yang menyerang sistem informasi melalui jaringan atau sarana teknis lainnya dengan menggunakan cacat konfigurasi, cacat protokol, cacat program, atau serangan kekerasan, yang menyebabkan masalah atau potensi kerusakan pada operasi sistem informasi. Peristiwa perusakan informasi terjadi ketika data di sistem informasi dirusak, dipalsukan, dibocorkan, atau dicuri oleh jaringan atau sarana teknis lainnya. Insiden keamanan konten informasi mengacu pada penggunaan jaringan informasi untuk mempublikasikan dan menyebarkan konten yang dapat mengancam stabilitas sosial, keamanan nasional, atau kepentingan publik. Kegagalan peralatan fasilitas mencakup peristiwa keamanan informasi yang disebabkan oleh penggunaan manusia daripada sarana teknis; ini juga mencakup kegagalan sistem informasi itu sendiri atau fasilitas pendukung periferal. Bencana mengacu pada peristiwa yang mengancam keamanan informasi yang menyebabkan kerusakan fisik pada sistem informasi akibat situasi yang tidak aman.

Untuk mengkategorikan peristiwa keamanan informasi, terutama diperhatikan tiga komponen: yaitu, pentingnya sistem informasi, kehilangan sistem, dan efek sosial. Sistem informasi sangat penting karena berdampak bisnisnya terhadap keamanan negara, ekonomi, kehidupan sosial, dan bisnis organisasi. Ini termasuk sistem informasi penting khusus, sistem

informasi penting umum, dan sistem informasi penting. Kerusakan sistem mengacu pada kerusakan yang terjadi pada keamanan informasi perangkat lunak, perangkat keras, fungsi, dan data sistem informasi, yang mengganggu layanan dan merusak organisasi. Kerusakan sistem dapat dikategorikan menjadi sangat serius, serius, besar, dan kecil. Dalam hal gangguan keamanan informasi yang berdampak pada masyarakat, istilah "dampak sosial" mengacu pada spektrum dan luasnya, dan dapat mencakup

Tabel 2. 1 Tingkatan darurat peristiwa keamanan informasi

Tingkat tanggap darurat	Deskripsi konten
Peristiwa Tingkat I	Serangan atau peristiwa keamanan yang signifikan atau kerusakan yang signifikan terhadap operasi bisnis pusat data telah terjadi, atau sistem operasi yang ada telah dimatikan selama kurang dari empat jam.
Peristiwa Tingkat II	Performa operasi sistem yang ada sangat menurun, performa jaringan tidak normal, atau peristiwa keamanan sangat memengaruhi layanan pusat data. Dan peristiwa tersebut berlangsung kurang dari 8 jam. Peristiwa yang berlangsung selama lebih dari 8 jam ditingkatkan ke level I
Peristiwa Tingkat III	Peristiwa yang mengganggu sistem dan keamanan informasi (seperti virus) terjadi dalam jumlah kecil, tetapi sebagian besar operasi bisnis masih dapat berjalan normal, dan peristiwa tersebut berlangsung kurang dari 8 jam. Peristiwa yang berlangsung lebih dari delapan jam dinaikkan ke Level II
Peristiwa Tingkat IV	Untuk fungsi, instalasi, atau konfigurasi perangkat penyimpanan, perangkat keamanan, dan perangkat keamanan, diperlukan konsultasi atau dukungan teknis. Peristiwa ini berlangsung kurang dari empat jam dan memengaruhi operasi layanan pusat data dengan sedikit atau tidak. Peristiwa yang berlangsung lebih dari empat jam naik ke level III

Dibagi menjadi dampak sosial yang sangat signifikan, dampak sosial yang signifikan, dampak sosial yang lebih besar, dan dampak sosial umum. Berdasarkan elemen- elemen di atas, kejadian keamanan informasi dapat dibagi menjadi empat tingkatan: kejadian yang sangat signifikan (I), kejadian besar (II), kejadian besar (III), dan kejadian umum (IV). Tingkat darurat insiden keamanan informasi ditunjukkan pada Tabel 2.1.

Kejadian level IV termasuk dalam kategori layanan pemeliharaan operasi harian, kejadian level III ditangani oleh personel pemeliharaan operasi harian, tetapi perlu diinformasikan kepada personel terkait tanggap darurat untuk kejadian level II dan I termasuk dalam kejadian tanggap darurat, kejadian dari level IV ditingkatkan ke level III, dan segera memberi tahu tim tanggap darurat oleh personel pemeliharaan operasi dan meluncurkan rencana tanggap darurat.

- **Mengaktifkan rencana tanggap darurat.** Organisasi akan dimasukkan ke dalam mode darurat setelah memulai rencana tanggap darurat. Prinsip awal, dasar awal, dan metode awal adalah tiga prinsip yang harus dipatuhi ketika memulai rencana tanggap darurat.

  Prinsip awal: Rencana tanggap darurat harus dimulai dengan cepat dan teratur. Ini berarti pemberitahuan tentang dimulainya rencana, kedatangan personel, penanganan kejadian, dan kedatangan sumber daya eksternal.

  Dasar awal: Untuk kejadian keamanan informasi yang mendadak atau penting, seperti gangguan layanan atau kerusakan sistem, segera mulai rencana tanggap darurat. Ada empat faktor yang dapat digunakan untuk memulai rencana tanggap darurat: jumlah kehilangan personel atau fasilitas; jumlah kehilangan sistem, termasuk kehilangan fisik, operasional, dan biaya; tingkat dampak sistem terhadap tujuan organisasi; dan durasi bisnis akhir yang diharapkan. Jika hasil penilaian kerusakan menunjukkan bahwa salah satu atau lebih kondisi aktivasi telah terpenuhi, rencana tanggap darurat akan diaktifkan.

  Metode memulai: Rencana tanggap darurat dimulai oleh kelompok pemimpin tanggap darurat. Setelah rencana tanggap darurat dibuat, kelompok pemimpin harus memeriksa dan memantau sumber daya manusia, keuangan, dan material yang tersedia. Mereka juga harus menyimpan catatan tentang kondisi saat ini.
- **Penanganan darurat:** Penanganan darurat dapat dimulai setelah rencana tanggap darurat dimulai dan dampak peristiwa keamanan informasi dikendalikan dengan baik. Penanganan darurat mencakup membangun kemampuan pemrosesan layanan sementara, seperti mengimpor data cadangan, memperbaiki sistem yang rusak, dan memulihkan kemampuan menjalankan layanan. Tiga komponen utama terlibat dalam pemulihan ini: urutan pemulihan, tugas pemulihan, dan proses pemulihan.

  Urutan pemulihan: Dalam proses analisis dampak layanan, urutan pemulihan ditetapkan sebagai prioritas utama fungsi layanan.

  Tugas pemulihan: Tugas pemulihan mencakup menginformasikan mitra bisnis internal dan eksternal mengenai sistem yang relevan, termasuk mereka yang terlibat dalam tanggap darurat dan personel yang relevan dari unit bisnis organisasi; mendapatkan otorisasi untuk mengakses peralatan yang rusak agar personel darurat dapat melakukan pekerjaan mereka; dan memperoleh persediaan dan tempat kerja darurat yang diperlukan, termasuk perangkat lunak dan data (seperti perangkat lunak siaga).

  Pasca-pemrosesan. Sebelum pemrosesan Rekonstruksi sistem informasi dan ringkasan tanggap darurat adalah bagian dari proses pemrosesan. Segera setelah tanggap darurat

untuk mengontrol keadaan, infrastruktur yang rusak harus segera diperbaiki dan operasi normal dimulai.

- **Rekonstruksi sistem**: Pertama, semua data harus dikumpulkan dan dianalisis secara statistik untuk mengidentifikasi faktor-faktor yang berkontribusi pada kecelakaan. Misalnya, Anda dapat mendapatkan informasi tentang jenis, luas, dan tingkat kerusakan sistem dengan mengumpulkan dan menganalisis log sistem, termasuk log deteksi intrusi dan konfigurasi. Kedua, kerugian dan efek yang ditimbulkan oleh insiden keamanan data serta kemampuan pemulihan dan rekonstruksi dievaluasi dan dievaluasi. Ketiga, buat rencana rekonstruksi sistem dan selesaikan pekerjaan dengan cepat. Terakhir, langkah-langkah yang diambil untuk mempersiapkan diri untuk "keadaan perang" berikutnya harus dievaluasi setelah rekonstruksi sistem selesai.

  Ringkasan tanggap darurat: Ini mencakup analisis dan ringkasan penyebab dan fenomena kejadian; menilai tingkat kerusakan dan kerugian pada sistem; menganalisis dan meringkas catatan tanggap darurat; menilai efektivitas dan efisiensi tindakan tanggap darurat; dan memberikan saran untuk perbaikan.

(5) Langkah-langkah jaminan tanggap darurat

Langkah-langkah jaminan tanggap darurat merupakan bagian penting dari rencana tanggap darurat keamanan informasi, dan merupakan komponen penting untuk memastikan implementasi rencana tanggap darurat yang cepat dan efektif setelah insiden keamanan informasi terjadi. Dukungan manusia, dukungan material, dan dukungan teknis adalah komponen utama dari tindakan jaminan tanggap darurat. Keamanan manusia adalah kunci dalam keseluruhan proses tanggap darurat keamanan informasi. Baik personel manajemen maupun personel teknis memiliki jaminan sumber daya manusia. Baik jaminan material dasar maupun tanggap darurat termasuk dalam jaminan material. Permintaan dukungan material dasar terkait dengan dukungan teknis dan manajemen harian; ini berarti bahwa dukungan teknis harus diselesaikan, pekerjaan manajemen harus diselesaikan, dan layanan teknis harus tersedia dalam tanggap darurat. Keuangan, dukungan transportasi, penjagaan keamanan publik, dan dukungan komunikasi adalah bantuan material untuk tanggap darurat. Untuk memastikan dana untuk tanggap darurat, diperlukan dukungan keuangan. Layanan dukungan teknis harian dan tanggap darurat tersedia. Tim dukungan teknis tanggap darurat bertanggung jawab atas dukungan teknis, menyelidiki dan mengawasi dasar teknis yang relevan, memilih penyedia layanan teknis yang sesuai, dan mendefinisikan tanggung jawab dan cara berkomunikasi.

(6) Lampiran

Rencana tanggap darurat yang paling penting tidak disertakan dalam lampiran. Ini biasanya mencakup: struktur organisasi dan tanggung jawab individu tertentu; informasi kontak tentang setiap anggota tim rencana tanggap darurat; informasi tentang pemasok dan titik kontak eksternal untuk penyimpanan keberangkatan dan stasiun siaga; daftar periksa dan prosedur pemulihan atau perawatan sistem; daftar persyaratan peralatan dan sistem untuk perangkat keras, perangkat lunak, dan sumber daya lain yang mendukung operasi sistem; dan prosedur penyimpanan dampak.

3. Latihan

Pelaksanaan rencana tanggap darurat meliputi uji coba, pelatihan, dan latihan rencana tanggap darurat serta penyimpanan, pendistribusian, dan pemeliharaan dokumen rencana tanggap darurat keamanan informasi.

Pengujian, pelatihan, dan latihan rencana tanggap darurat. Untuk menguji keefektifan rencana tanggap darurat, dan membuat personel yang relevan untuk memahami tujuan rencana dan proses tanggap darurat keamanan informasi, memahami pengoperasian prosedur tanggap darurat, perdagangan elektronik perusahaan rencana tanggap darurat harus sesuai dengan persyaratan berikut pengujian, pelatihan, dan latihan: Termasuk rencana pengujian, pelatihan, dan latihan terlebih dahulu di tempat pengujian, pelatihan, dan gladi bersih; Seluruh proses pengujian, pelatihan, dan latihan harus dicatat secara rinci dan dilaporkan; Pengujian, pelatihan, dan latihan tidak boleh mengganggu operasi bisnis normal sistem informasi; , pelatihan, dan latihan lengkap dengan partisipasi pengguna akhir harus diselesaikan setidaknya setahun sekali. Selain itu, rencana darurat perlu diperbarui secara tepat waktu, karena strategi bisnis organisasi akan berubah, teknologi akan diperbarui, atau kebijakan akan berubah. Latihan dan pembaruan rencana dapat digabungkan, dan hasil latihan dan pelajaran yang didapat, serta informasi untuk meningkatkan efisiensi, dapat ditambahkan ke dalam rencana tanggap darurat.

Menyimpan, mendistribusikan, dan memelihara dokumen rencana tanggap darurat keamanan informasi. Untuk dokumen rencana tanggap darurat yang telah ditinjau dan disetujui, hal-hal berikut ini harus dilakukan: Memiliki beberapa salinan dan disimpan di lokasi yang berbeda; Didistribusikan kepada semua personel yang terlibat dalam tanggap darurat; Memperbarui semua salinan secara seragam setelah setiap revisi; Versi lama harus dimusnahkan sesuai dengan peraturan yang relevan; Dan seterusnya. Untuk memastikan efektivitas rencana tanggap darurat, dokumen rencana tanggap darurat harus dipelihara dari beberapa aspek berikut: Pertama, perubahan proses bisnis, sistem informasi, dan personel harus

tercermin dalam dokumen rencana tanggap darurat tepat waktu; Kedua, uji coba dan latihan rencana tanggap darurat serta proses implementasi aktual setelah terjadinya insiden keamanan informasi harus dicatat secara rinci, dan pengaruhnya harus dievaluasi; Ketiga, dokumen rencana tanggap darurat harus ditinjau dan direvisi secara teratur.

2.4.3 Konstruksi DRP untuk Manajemen Keamanan E-commerce

Rencana pemulihan bencana manajemen keamanan e-commerce (selanjutnya disebut rencana pemulihan bencana) mengacu pada rencana dan pengaturan sebelumnya yang dibuat untuk mengurangi kerugian perusahaan e-commerce yang disebabkan oleh peristiwa bencana dan memastikan bahwa fungsi bisnis utama yang didukung oleh sistem e-commerce dapat dipulihkan secara tepat waktu dan terus beroperasi setelah bencana terjadi. Untuk mengatasi kejadian bencana dengan lebih baik, perusahaan e- commerce harus membuat rencana pemulihan bencana. Perusahaan e-commerce dapat membuat rencana pemulihan bencana sendiri, dengan mempekerjakan ahli eksternal yang berkualifikasi untuk mendapatkan panduan, atau dengan mempercayakan organisasi eksternal yang berkualifikasi.

Perumusan rencana pemulihan bencana untuk manajemen keamanan e-commerce meliputi tiga tahap: persiapan, perencanaan, dan praktik.

1. Preparasi

Tentukan persyaratan untuk pemulihan bencana, membuat strategi pemulihan bencana, dan menerapkannya adalah semua bagian dari pembuatan rencana pemulihan bencana.

(1) Determinasi kebutuhan

Analisis risiko, analisis dampak bisnis, dan tujuan pemulihan bencana adalah dasar untuk menentukan kebutuhan pemulihan bencana. Lihat 2.4.2 untuk informasi tentang analisis risiko, analisis dampak bisnis, dan penentuan target pemulihan bencana.

(2) Kontruksi strategi

Analisis biaya-manfaat harus menjadi dasar dari pendekatan pemulihan bencana. Berdasarkan tujuan pemulihan bencana yang ditetapkan dalam analisis dampak bisnis, pemulihan bencana. Prinsip keseimbangan risiko menentukan kebijakan untuk setiap operasi bisnis utama. Ini berarti bahwa kerugian yang disebabkan oleh risiko harus diimbangi dengan biaya sumber daya yang diperlukan untuk pemulihan bencana. Banyak fungsi bisnis utama dapat memiliki kebijakan pemulihan bencana yang berbeda. Semua sumber daya yang diperlukan untuk tingkat kemampuan pemulihan bencana (sistem cadangan data, cadangan, sistem jaringan cadangan, infrastruktur sistem pemrosesan data cadangan, dukungan teknis profesional, pemeliharaan dan manajemen operasi, rencana pemulihan bencana) harus

termasuk akses dan tingkat kemampuan pemulihan bencana (tingkat dukungan dasar, tingkat dukungan situs cadangan, tingkat transmisi elektronik, dan dukungan perangkat lunak).

(3) Strategi diterapkan

Strategi pemulihan bencana harus mencakup rencana teknis untuk sistem cadangan bencana, serta proses pemilihan dan pembangunan pusat cadangan bencana.

- **Skema teknis sistem cadangan bencana.**

Buatlah rencana teknis sistem cadangan bencana yang sesuai dengan strategi pemulihan bencana. Ini harus mencakup rencana untuk sistem cadangan data, sistem pemrosesan data, dan sistem jaringan. Departemen terkait dalam organisasi harus mengonfirmasi dan memverifikasi solusi teknis, dan mencatat dan menyimpan hasil verifikasi dan verifikasi untuk memastikan bahwa solusi teknis memenuhi persyaratan kebijakan pemulihan bencana. Terapkan sistem cadangan data yang diperlukan, sistem pemrosesan data cadangan, dan sistem jaringan cadangan sesuai dengan skema teknis sistem cadangan bencana yang telah dikonfirmasi; buat rencana instalasi dan pengujian yang mendukung setiap operasi bisnis utama; dan atur pengguna akhir untuk menguji bersama.

- **Pemilihan dan pembangunan pusat cadangan bencana.**

Persyaratan dasar: Berdasarkan hasil analisis risiko, saat memilih atau membangun pusat cadangan bencana, pastikan bahwa pusat cadangan bencana dan pusat utama tidak terpapar risiko yang sama. Untuk mengurangi risiko bencana di wilayah yang berbeda, Anda dapat memilih pusat pencadangan bencana yang berada di kota yang sama atau jauh. Pusat pencadangan bencana harus memiliki sumber daya komunikasi dan daya yang diperlukan untuk pencadangan dan pemulihan data, serta rute transportasi yang nyaman untuk personel dan peralatan pemulihan bencana. Prinsip perencanaan keseluruhan, pembagian sumber daya, dan integrasi harus mengatur pusat pencadangan bencana secara rasional.

Persyaratan infrastruktur: Infrastruktur pusat pencadangan bencana harus memenuhi tujuan pemulihan bencana dan persyaratan standar nasional yang relevan.

Persyaratan kemampuan dukungan teknis: Menurut kebijakan pemulihan bencana, perusahaan e-commerce harus memiliki kemampuan untuk menyediakan dukungan teknis profesional untuk sistem pencadangan bencana. Pusat pencadangan bencana harus memiliki organisasi dukungan teknis dan personel yang bertanggung jawab untuk dukungan teknis harus dilatih secara teratur.

Kemampuan manajemen operasi dan pemeliharaan: untuk mencapai tujuan pemulihan bencana, berbagai prosedur operasi dan sistem manajemen harus diterapkan untuk pusat

pencadangan bencana. Ini termasuk memastikan bahwa sistem pemrosesan data siaga dan sistem jaringan siaga dalam keadaan normal dan konsisten dengan parameter sistem utama, meningkatkan ketepatan waktu dan efektivitas pencadangan data, serta meningkatkan tanggap darurat dan kapasitas pemrosesan.

2. Perencanaan

Dokumen rencana pemulihan bencana terdiri dari tujuh bagian: peraturan umum dan tanggung jawab, prosedur tanggap darurat, pemulihan dan pengoperasian kembali, rekonstruksi dan pengembalian pasca bencana, ketentuan jaminan, dan lampiran.

(1) Regulasi umum

Rencana pemulihan bencana biasanya menjelaskan istilah dan metode yang digunakan dalam rencana pemulihan bencana, serta tujuan pemulihan bencana, termasuk tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO). Bagian ini menjelaskan tujuan dan lingkup rencana pemulihan bencana. Ini mencakup operasi harian pusat pencadangan bencana, pemulihan dan pengaktifan kembali fungsi layanan utama, rekonstruksi dan pengaktifan kembali sistem utama, dan tindakan tanggap darurat setelah keadaan darurat. Selain itu, mereka memberikan penjelasan tentang bagaimana rencana pemulihan bencana menyelesaikan masalah tersebut.

(2) Organisasi dan tanggung jawab

Bagian organisasi dan tanggung jawab menjelaskan organisasi pemulihan bencana, tanggung jawab pekerjaan, dan daftar staf. Tanggap darurat dan tim pemulihan bencana biasanya merupakan bagian dari organisasi pemulihan bencana. Anda dapat membentuk kelompok pemulihan bencana untuk pemimpin, implementasi, dan operasi harian. Organisasi terdepan dalam pemulihan bencana adalah grup pemimpin pemulihan bencana, dan anggota pemimpinnya harus termasuk dalam manajemen puncak perusahaan e-commerce. Membuat keputusan tentang masalah penting pemulihan bencana adalah tanggung jawab kelompok pemimpin pemulihan bencana. Ini termasuk pemeriksaan dan persetujuan rencana pemulihan bencana, anggaran dana, pemeriksaan dan persetujuan pelaksanaan rencana, dan hal-hal lainnya. Melakukan analisis kebutuhan pemulihan bencana, membuat strategi pemulihan bencana, membuat rencana pemulihan bencana, dan merencanakan pengujian, pelatihan, dan latihan rencana pemulihan bencana adalah tugas utama tim implementasi rencana pemulihan bencana. Salah satu tugas utama tim operasi harian adalah pemulihan bencana. Tugas ini mencakup membantu implementasi rencana pemulihan bencana, manajemen harian pusat pemulihan bencana, menjalankan dan memelihara sistem pemulihan bencana, dukungan teknis profesional pemulihan bencana, partisipasi dan membantu dalam pendidikan dan pelatihan

rencana pemulihan bencana, pelatihan dan latihan, pemeliharaan dan pengelolaan rencana pemulihan bencana, dan penilaian kerus setelah peristiwa bencana terjadi. Perusahaan e-commerce dapat mempekerjakan pakar eksternal untuk membantu melaksanakan pemulihan bencana, atau mempercayakan perusahaan eksternal dengan kualifikasi yang sesuai untuk melakukan sebagian atau seluruh pekerjaan tim implementasi dan operasi harian.

(3) Metode tanggap darurat

Pemberitahuan kejadian, evakuasi, penilaian kerusakan, dan deklarasi bencana adalah empat langkah dalam proses tanggap bencana.

- **Pemberitahuan tentang peristiwa**. Ketika personel mengetahui bahwa keadaan darurat sistem informasi telah terjadi atau akan terjadi, mereka harus melaporkannya sesuai dengan proses yang telah ditetapkan, dan personel yang terkait harus melakukan penilaian awal, pemberitahuan, dan pembuangan.
- **Evakuasi** Tentukan metode evakuasi, rencana, prosedur, dan lainnya, dan sediakan.
- **Penilaian kerusakan**. Setelah keadaan darurat terjadi, anggota tim tanggap darurat yang menilai kerusakan harus menentukan seberapa parah keadaan. Setelah itu, orang yang bertanggung jawab atas pemulihan bencana harus menghubungi profesional terkait untuk menilai keadaan darurat secara menyeluruh, mengevaluasi dampak keadaan darurat pada sistem, dan menentukan tindakan selanjutnya yang harus diambil.
- **Deklarasi bencana**. Menetapkan kondisi untuk rencana pemulihan bencana untuk memulai terlebih dahulu. Setelah hasil penilaian kerusakan mencapai satu atau lebih dari situasi awal, tim tanggap darurat secara resmi mengeluarkan deklarasi bencana, mengaktifkan rencana pemulihan bencana, dan memberi tahu departemen terkait.

(4) Pemulihan dan pengoperasian kembali

- **Pemulihan**. Sistem pemulihan data, pemrosesan data, dan jaringan yang mendukung fungsi layanan utama pusat pencadangan bencana disebut pemulihan. Prioritas pemulihan fungsi layanan utama ditentukan dalam analisis dampak layanan. Pada bagian ini, waktu penting, lokasi, personel, peralatan, dan langkah-langkah operasi yang digunakan selama proses pemulihan dijelaskan. Ada juga instruksi tentang cara berkoordinasi dengan tim jika bencana terjadi, dan prosedur untuk menangani pengecualian.
- **Pengoperasian kembali**. Pengoperasian ulang adalah mengganti sistem utama yang mengalami bencana sistem pusat pencadangan yang digunakan untuk memulihkan operasi bisnis yang penting. Semua prosedur operasional dan peraturan untuk memulai kembali operasi dijelaskan di bagian ini.

(5) Perbaikan dan pemulihan setelah bencana

Rekonstruksi dan rollback pasca-bencana adalah istilah yang mengacu pada gangguan sistem cadangan bencana untuk kembali ke sistem utama dan rekonstruksi pusat utama, yang merupakan pusat data tempat sistem utama, pusat produksi, dan situs utama berada. Proses pemulihan dan pengembalian bencana dibahas dalam bagian ini.

(6) Syarat jaminan

Dukungan teknis profesional, dukungan komunikasi, dukungan logistik, dan hal-hal lainnya adalah bagian dari kewajiban jaminan.

(7) Lampiran

Orang-orang dan organisasi yang terkait dengan pemulihan bencana (seperti tim pemulihan bencana, operator, vendor, departemen, media, dll.) termasuk dalam lampiran. Ini termasuk tabel kontak, rencana evakuasi, manual produk, perjanjian dan memorandum tingkat layanan, daftar sumber daya, laporan analisis dampak bisnis, rencana, pelestarian, dan metode distribusi.

3. Latihan

Praktik rencana pemulihan bencana mencakup pengujian, pelatihan, dan latihan rencana pemulihan bencana, serta penyimpanan, distribusi, dan pemeliharaan dokumen rencana pemulihan bencana. Untuk detailnya, lihat konten yang relevan di 2.4.2.

2.4.4 Konstruksi BCP untuk Manajemen Keamanan *E-Commerce*



Gambar 2.3 Konstruksi BCP untuk Manajemen Keamanan *E-Commerce*

Manajemen keamanan e-commerce memiliki rencana keberlangsungan bisnis, yang juga disebut sebagai rencana keberlangsungan bisnis, yang mencakup berbagai strategi dan rencana yang telah dibuat sebelumnya. Ini adalah mekanisme untuk mencegah dan menangani bencana. Hal ini memungkinkan operasi utama perusahaan e-commerce tetap berjalan saat bencana terjadi, memastikan kelangsungan bisnis. Penyusunan, persiapan, dan pelaksanaan

rencana kesinambungan bisnis mirip dengan rencana pemulihan bencana dan tanggap darurat. Untuk materi terkait, lihat 2.4.2 dan 2.4.3. Dalam rencana keberlangsungan bisnis, strategi keberlangsungan bisnis dibahas di bawah ini.

1. Konstruksi strategi

Strategi keberlangsungan bisnis adalah bagian penting dari perencanaan keberlangsungan bisnis dan dibangun berdasarkan penilaian risiko dan analisis dampak bisnis. Kebijakan pencegahan, respons, kelangsungan, pemulihan, dan pemulihan layanan adalah semua contoh kebijakan kelangsungan bisnis.

Strategi pencegahan termasuk strategi pengendalian pencegahan dan pengendalian pencegahan; keduanya bertujuan untuk mengurangi kemungkinan bencana. Area yang lemah perusahaan dilindungi dengan strategi pengendalian pencegahan untuk mengurangi risiko dan dampaknya.

Perencanaan pemulihan dan prosedur notifikasi siapa yang perlu diberitahu, bagaimana, dan oleh siapa adalah strategi respons. Rencana keberlanjutan bisnis harus mencakup pohon notifikasi sehingga pesan dikirimkan pertama ke satu kelompok, kemudian ke kelompok lain, dan seterusnya. Semua orang yang terdaftar dalam pohon notifikasi memiliki tugas dan posisi yang berbeda. Ini adalah anggota dari berbagai tim, seperti manajemen, penilaian risiko, tim teknis, dan tim operasi, antara lain.

Kebijakan kontinuitas tidak berlaku untuk semua layanan; hanya layanan yang sensitif terhadap waktu baik segera setelah gangguan atau dalam jangka waktu yang dapat diterima setelah gangguan yang dimaksudkan untuk diterapkan. Layanan yang tidak sensitif terhadap waktu dapat pulih dengan menggunakan kebijakan pemulihan layanan. Waktu mulai pemulihan bisnis bervariasi tergantung pada seberapa lama bisnis harus beroperasi. Saat melakukan pemulihan bisnis, Anda harus memulihkan tempat kerja (mungkin tempat kerja utama atau tempat kerja alternatif), sistem operasi pada perangkat cadangan, dan sistem aplikasi yang diperlukan sesuai dengan pemulihan ShuXu tertentu. Kemudian, Anda harus memulihkan sistem operasi dari cadangan, memulihkan sistem aplikasi yang diperlukan dalam urutan tertentu, dan kemudian mengembalikan data dari media cadangan data. Penting untuk diingat bahwa data yang dipulihkan harus sesuai dengan data pada tanggal yang telah ditentukan sebelum gangguan layanan. Persyaratan fungsi layanan utama menentukan pemilihan titik waktu.

Salah satu bagian dari strategi pemulihan adalah perbaikan dan pemulihan fasilitas utama, yang pada akhirnya akan mengembalikan keseluruhan operasi perusahaan. Pemulihan bisnis diperlukan jika tempat kerja asli tidak dapat diperbaiki setelah bencana.

2. Implementasi strategi

Untuk menerapkan strategi kelangsungan usaha, Anda harus membentuk tim yang sesuai dan membuat rencana penerapan untuk kelangsungan usaha; menerapkan pengaturan cadangan; menerapkan strategi mitigasi risiko; dan menerapkan kebijakan kelangsungan usaha.

Sebagian besar organisasi menggabungkan rencana keberlangsungan bisnis dan pemulihan bencana, karena keduanya terkait erat. Operasi pembangunan kembali sistem di berbagai lokasi mulai dari lokasi cadangan hingga kembali ke tempat kerja utama harus dapat dilakukan oleh rencana gabungan tersebut. Oleh karena itu, meskipun rencana keberlanjutan bisnis dan pemulihan bencana dapat digabungkan menjadi satu rencana saat dikembangkan, implementasinya membutuhkan tim pelaksana yang berbeda.

BAB 3
Manajemen Keamanan *E-commerce*: Sumber Daya dan Organisasi

Pengembangan e-commerce membutuhkan keamanan, dan sumber daya dan organisasi adalah dasar dan jaminan penting untuk penerapan manajemen keamanan e-commerce. Saat melakukan bisnis e-commerce, kita harus memprioritaskan pengembangan sumber daya dan penerapan manajemen keamanan.

3.1 Hubungan Sumber Daya dan Organisasi Manajemen Keamanan *E-commerce*

Karena skala e-commerce yang terus berkembang, masalah keamanan e-commerce semakin serius. Untuk mencapai tujuan manajemen keamanan e-commerce, perlu ada alokasi sumber daya dan organisasi yang bijak dan logis.

3.1.1 Definisi Sumber Daya dan Organisasi Manajemen Keamanan *E-commerce*

1. Definisi sumber daya dan organisasi manajemen keamanan e-commerce.

Sumber daya manajemen keamanan e-commerce sangat penting bagi perusahaan e-commerce untuk mencapai tujuan dan melakukan aktivitas terkait. Ini menempati bagian tertentu dari sumber daya perusahaan, yang dipengaruhi oleh tujuan strategis keamanan e-commerce, skala, bisnis, kekuatan, dan kesadaran manajemen.

Menurut berbagai standar, sumber daya manajemen keamanan e-commerce dapat dibagi menjadi berbagai jenis, tergantung pada fungsinya. Sumber daya manusia, teknis, keuangan, informasi, dan budaya adalah beberapa jenis sumber daya manajemen keamanan e-commerce, yang dijelaskan secara rinci di Bagian 3.2.1. Menurut jenis sumber daya, sumber daya dapat dibagi menjadi sumber daya internal dan sumber daya eksternal. Sumber daya internal terdiri dari berbagai sumber daya yang dapat dikontrol dan dikendalikan langsung oleh organisasi. Ini termasuk sumber daya keuangan, sumber daya material, sumber daya informasi, sumber daya hubungan, sumber daya budaya, sumber daya pelanggan, strategi, kebijakan, dan sistem. Sumber daya industri, sumber daya industri, sumber daya pasar, dan sumber daya lingkungan eksternal adalah contoh sumber daya eksternal yang berkaitan erat dengan aktivitas organisasi. Sumber daya eksternal ini tidak secara langsung dikendalikan oleh organisasi, tetapi memiliki dampak yang signifikan terhadap aktivitas organisasi. Karena perbedaan pengetahuan dan kemampuan, berbagai organisasi mungkin tidak melakukan cara yang sama untuk memperoleh dan memanfaatkan sumber daya. Sumber daya organisasi dapat dibagi menjadi sumber daya berwujud dan sumber daya tidak berwujud. Sumber daya berwujud biasanya mencakup sumber daya yang ada dalam bentuk fisik, seperti sumber daya alam, bangunan, mesin dan peralatan,

produk fisik, modal, personil, dan lain-lain, yang penting bagi organisasi untuk bertahan hidup dan berkembang.

2. Pengertian manajemen keamanan e-commerce bagi organisasi

Di satu sisi, organisasi adalah kelompok orang yang bekerja untuk tujuan tertentu, sebuah sistem dengan tujuan yang jelas, struktur yang baik, dan kegiatan yang terkoordinasi, mirip dengan perusahaan. Sebaliknya, manajemen adalah proses pembagian sumber daya di antara individu atau di antara individu dan benda-benda.

Selain itu, organisasi manajemen keamanan e-commerce memiliki makna dalam dua aspek: organisasi manajemen keamanan e-commerce dan fungsi manajemen keamanan e-commerce. Organisasi manajemen keamanan perdagangan elektronik yang ideal mencakup hal-hal berikut: Ada tujuan yang jelas untuk melindungi bisnis dari kerugian; Ada orang yang bertanggung jawab untuk mengelola keamanan; dan ada aturan dan struktur sistem yang sesuai untuk mengawasi dan mengatur tindakan anggota, seperti sistem manajemen keselamatan, pengaturan pos, atau aturan. Organisasi manajemen keamanan e-commerce adalah semua organisasi yang disebutkan dalam bab ini, kecuali yang disebutkan secara khusus.

Pengorganisasian kegiatan tidak hanya bertujuan untuk mengumpulkan kekuatan individu; itu juga bertujuan untuk mengumpulkan dan memperkuat kekuatan individu dengan cara yang menghindari pembatalan timbal balik. Organisasi manajemen keamanan e-commerce adalah serangkaian tindakan yang dilakukan untuk memaksimalkan manfaat melalui penggunaan sumber daya manusia, keuangan, material, dan sumber daya lainnya. Ini memiliki sifat konvergensi, amplifikasi, dan pertukaran. Konsep konvergensi mengacu pada kemampuan seseorang untuk organisasi untuk mengumpulkan orang-orang dari tempat yang berbeda dan melakukan pekerjaan bersama sebagai "kelompok". Amplifikasi: Efek yang, berdasarkan konvergensi, "keseluruhan lebih besar daripada jumlah bagian-bagiannya" disebut sebagai amplificasi. Pertukaran: Istilah "pertukaran" mengacu pada hubungan yang saling melengkapi antara individu dan kelompok yang didasarkan pada pertukaran yang setara.

3.1.1 Hubungan Antara Sumber Daya Manajemen Keamanan E-commerce dan Organisasi

Berikut ini adalah hubungan antara sumber daya manajemen keamanan e-commerce dan organisasi.

Pertama, sumber daya adalah dasar bagi kelangsungan hidup dan perkembangan organisasi. Kelangkaan sumber daya dan ketidakterawatan lingkungan menyebabkan

organisasi mengejar lebih banyak sumber daya untuk melindungi kepentingan mereka sendiri dan mengurangi dan menghindari dampak perubahan lingkungan.

Kedua, aktivitas manajemen memastikan alokasi dan penggunaan sumber daya dilakukan. Perencanaan, pengorganisasian, koordinasi, pengendalian, komunikasi, pengambilan keputusan, operasi, hubungan masyarakat, dan kegiatan lainnya adalah contoh pekerjaan manajemen. Untuk meningkatkan efisiensi manajemen, manajemen harus melakukan tindakan ini. Organisasi menggunakan kegiatan manajemen untuk mengintegrasikan sumber daya yang terbatas melalui seluruh proses pembagian sumber daya.

Ketiga, keduanya mempengaruhi satu sama lain dan berfungsi sama baiknya. Bagaimana sumber daya dialokasikan dan digunakan dipengaruhi oleh struktur organisasi. Misalnya, dalam "struktur piramida", karyawan dasar harus melalui berbagai lapisan persetujuan untuk mendapatkan sumber daya tertentu; namun, dalam "struktur datar", proses karyawan dasar untuk mendapatkan sumber daya dari jarak jauh lebih mudah. Pada saat yang sama, kuantitas, kualitas, dan jenis sumber daya juga akan mempengaruhi bagaimana suatu organisasi beroperasi. Misalnya, sebuah perusahaan harus membuat struktur yang rumit untuk mengalokasikan dan menggunakan sumber dayanya secara efektif jika mereka memiliki banyak sumber daya.

3.2 Sumber Daya Manajemen Keamanan E-commerce

Untuk bertahan dan berkembang, organisasi manajemen keamanan e-commerce membutuhkan beberapa sumber daya. Salah satu komponen utama manajemen organisasi adalah sumber daya. Organisasi tidak hanya mampu memperoleh sumber daya yang tepat, tetapi juga mampu mengalokasinya secara efisien.

1. Komposisi sumber daya manajemen keamanan e-commerce

Seperti yang telah disebutkan di atas, dari sudut pandang fungsi sumber daya, sumber daya manajemen keamanan e-commerce terutama terdiri dari sumber daya manusia. Organisasi manajemen keamanan e-commerce juga berbeda dalam jenis, kuantitas, dan kualitas sumber daya yang mereka miliki.

Sumber daya manusia adalah jenis sumber daya yang paling penting dan harus dimiliki oleh setiap organisasi. Sebuah organisasi hanya dapat menangani berbagai ancaman keamanan internal dan eksternal dengan tim manajemen keamanan yang baik. Kepala petugas keamanan, pengawas keamanan, administrator keamanan, analis keamanan, teknisi keamanan, konsultan keamanan, staf layanan pelanggan, staf hukum, auditor, personel keamanan, dll. Kepala petugas keamanan terutama bertanggung jawab atas operasi yang aman dari seluruh perusahaan

e-commerce, serta evaluasi dan manajemen proyek manajemen keamanan e-commerce. Teknisi keamanan bertanggung jawab atas pekerjaan teknis keamanan tertentu dan memiliki kualifikasi teknis tertentu. Konsultan keamanan berpengalaman dalam mengelola keamanan e-commerce. Petugas keamanan bertani adalah orang-orang yang memiliki keahlian hukum untuk memastikan bahwa strategi dan operasi khusus perusahaan e-commerce adalah legal dan patuh. Auditor bertanggung jawab untuk menyusun rencana audit, melaksanakan pekerjaan audit, mengawasi, memeriksa, dan mengevaluasi aktivitas bisnis dan keuangan perusahaan e-commerce. Staf layanan pelanggan dapat membantu tim manajemen keamanan e-bisnis mengidentifikasi potensi masalah keamanan. Secara alami, manajemen keamanan e-commerce bergantung pada sumber daya teknis, terutama penerapan big data dan teknologi kecerdasan buatan, yang menawarkan metode dan pendekatan baru untuk manajemen keamanan.

Sumber daya teknis termasuk teknologi lunak, teknologi perangkat keras, paten, produk keamanan, dan sumber daya lainnya yang dimiliki oleh organisasi. Namun, ada manajer yang akan aman dalam berbagai perangkat lunak atau perangkat keras keamanan, dan mengabaikan pentingnya manajemen, menghasilkan banyak peralatan keamanan tetapi dampak keamanannya buruk.

Sumber daya keuangan mengacu pada jumlah modal atau uang tunai yang dimiliki oleh organisasi yang dapat digunakan dalam kegiatan manajemen keamanan e-commerce. Sumber daya informasi mengacu pada jumlah sumber daya informasi yang dimiliki oleh organisasi yang dapat digunakan dalam kegiatan manajemen keamanan e-commerce. Sumber daya keuangan, sampai batas tertentu, mencerminkan jumlah sumber daya yang dimiliki oleh organisasi, yang penting untuk memastikan bahwa penerapan manajemen keamanan Jenis data tertentu disebut informasi. Data telah melonjak karena diversifikasi dan kemudahan akses, terutama di bidang e-commerce. Meskipun mendapatkan sumber daya seperti itu lebih mudah daripada sebelumnya, hal ini membutuhkan kemampuan tata kelola data organisasi yang lebih baik. Organisasi harus menghilangkan hambatan informasi, mengurangi pulau-pulau informasi, dan menghindari pengungkapan data privasi selama proses pengambilan dan penggunaan sumber daya data. Selama proses manajemen organisasi, sumber daya budaya, termasuk struktur budaya, nilai-nilai, kesadaran kelompok, dan sistem organisasi, adalah sumber daya yang tidak dapat dipertukarkan. Sumber daya budaya adalah sumber daya lunak yang sangat penting bagi sebuah organisasi, yang terdiri dari kesadaran dan kenyataan. Sumber daya budaya manajemen keselamatan e-commerce mencakup konsep keselamatan, perilaku keselamatan, manajemen keselamatan (sistem), bentuk material, dll., yang berfungsi untuk mengkonsolidasikan teori, standarisasi perilaku, dan orientasi kognisi.

Selain sumber daya yang disebutkan di atas, sumber daya material dan hubungan juga sangat penting bagi sumber daya dasar organisasi. Meskipun sumber daya ini tidak bergantung satu sama lain, mereka berinteraksi satu sama lain dan membentuk satu kesatuan organik.

2. Keterbatasan sumber daya manajemen keamanan e-commerce

Pertama, organisasi harus sepenuhnya mengembangkan dan memanfaatkan sumber daya ini, memaksimalkan nilainya melalui manajemen dan optimalisasi ilmiah yang berkelanjutan. Sumber daya organisasi terbatas, dan mereka bekerja baik karena pemahaman organisasi tentang manajemen keamanan dan kemampuan manajemennya. Keterbatasan sumber daya memengaruhi tujuan manajemen keamanan organisasi. Sumber daya yang tersedia untuk manajemen keamanan harus digunakan oleh organisasi untuk menentukan tujuan manajemen keamanan perdagangan elektronik.

Kedua, sumber daya yang tidak valid mungkin ada. Sumber daya manajemen keamanan organisasi mungkin tidak semuanya efektif karena beberapa sumber daya sudah usang dan tidak dapat digunakan lagi.

Ketiga, pemborosan sumber daya yang dialokasikan. Organisasi harus mengatur sumber daya yang terbatas untuk tugas atau kegiatan tertentu sehingga mereka dapat memaksimalkan output.

Dengan sumber daya yang diberikan, atau dengan meminimalkan sumber daya yang diberikan. Sumber daya dialokasikan untuk aktivitas atau kegiatan ini. Sumber daya dihabiskan saat dialokasikan.

3.2.1 Konfigurasi Sumber Daya Manajemen Keamanan E-Commerce

Organisasi harus mengatur dan memanfaatkan sepenuhnya sumber daya manajemen keamanan e-commerce untuk memenuhi tujuan manajemen keamanan

1. Konsep alokasi sumber daya manajemen keamanan e-commerce

Alokasi sumber daya manajemen keamanan e-commerce mengacu pada pencocokan berbagai jenis sumber daya dalam hal kuantitas dan kualitas sesuai dengan tujuan yang diteta. Sumber daya manusia memainkan peran penting dalam proses alokasi sumber daya dalam manajemen keamanan e-commerce karena pengetahuan, pengalaman, dan keterampilannya yang luas. Selain itu, tidak seperti sumber daya organisasi lainnya, sumber daya manusia merupakan variabel dalam alokasi sumber daya karena pengetahuan, pengalaman, dan keterampilannya yang kaya.

2. Mekanisme alokasi sumber daya manajemen keamanan e-commerce

Organisasi biasanya bergantung pada mekanisme administratif untuk alokasi sumber daya dalam manajemen perdagangan elektronik. Mekanisme ini terutama berkaitan dengan penggunaan organ administratif birokrasi untuk menjamin alokasi sumber daya berjalan dengan baik melalui perintah, eksekusi, inspeksi, dan pengawasan. Kelebihan dari mode konfigurasi ini adalah informasi atas dan bawah dapat dikomunikasikan dengan mudah, dan konfigurasi sumber daya dapat dilakukan dengan lebih efisien. Selain itu, hierarki yang ketat memastikan penentuan posisi tujuan organisasi dan pembagian kerja yang efektif. Di sisi lain, hierarki memungkinkan penggunaan sumber daya secara terpusat untuk meningkatkan efisiensi.

3. Konfigurasi Personel

Seperti yang disebutkan sebelumnya, sumber daya manusia memainkan peran penting dalam bagaimana sumber daya didistribusikan dalam sebuah organisasi. Hanya alokasi karyawan yang masuk akal yang dapat membuat perusahaan beroperasi dengan baik. Setiap posisi di perusahaan harus memiliki karyawan yang tepat untuk menjalankan semua tugas.

(1) Prinsip alokasi personel

Prinsip dasar alokasi personel adalah memilih orang sesuai dengan kebutuhan jabatan, meminta mereka untuk melakukan pekerjaan yang dibutuhkan oleh jabatan, dan memastikan bahwa mereka memiliki pengetahuan dan kemampuan yang sesuai. Prinsip dasar alokasi personel juga adalah memilih orang sesuai dengan situasi.

Prinsip keseimbangan personel yang dinamis: Ketika organisasi berkembang secara berkelanjutan, alokasi orang (personel) dan hal-hal (pekerjaan) juga perlu disesuaikan secara konstan untuk memungkinkan personel yang kompeten untuk berpartisipasi dalam pekerjaan sepenuhnya.

(2) Tentukan jenis dan jumlah staf

Jenis dan jumlah staf yang digunakan oleh organisasi di berbagai industri untuk membentuk departemen, posisi, dan staf manajemen keamanan. Untuk bisnis internet yang membutuhkan lebih dari 1000 set peralatan untuk manajemen keamanan, diperlukan 1-2 manajer keamanan penuh waktu (misalnya kepala petugas keamanan informasi), 3-4 administrator keamanan penuh waktu atau teknisi keamanan, 3-4 pengawas keamanan paruh waktu, dan 10-12 administrator keamanan paruh waktu. Jika jumlah perangkat yang perlu dikelola antara 100 dan 1000, Anda dapat mengonfigurasi satu administrator keamanan penuh waktu atau teknisi keamanan.

(3) Pemilihan karyawan

Karyawan harus dipilih untuk memastikan mereka memiliki pengetahuan dan keterampilan yang diperlukan. Orang yang disaring harus memiliki pengetahuan dan keterampilan yang sesuai, baik dari dalam maupun luar perusahaan.

(4) Pelatihan personel

Tidak diragukan lagi, pelatihan personel sangat penting dalam kepegawaian. Ini terutama berlaku untuk pelatihan personel manajemen. Tugas-tugas ini membutuhkan pengembangan pribadi karyawan dan perubahan teknologi. Oleh karena itu, penggunaan metode ilmiah, pelatihan yang terorganisir, terfokus, terencana, dan disesuaikan dengan karakteristik personel, dan beberapa pelatihan untuk semua personel dan beberapa pelatihan untuk personel tertentu.

4. Alokasi sumber daya dalam manajemen proyek

Manajemen dan proyek tidak dapat dipisahkan satu sama lain. Manajer proyek merencanakan, mengorganisir, memimpin, mengendalikan, dan menilai seluruh proses dari awal keputusan investasi hingga akhir proyek dengan sumber daya terbatas dengan menggunakan teori, perspektif, dan metode teori sistem untuk mencapai tujuan proyek. Dalam manajemen proyek, persyaratan sumber daya harus didefinisikan, kendala sumber daya harus dinilai, dan rencana alokasi sumber daya harus dibuat sesuai dengan persyaratan dan kendala sumber daya. Organisasi mengelola sumber daya berdasarkan rencana alokasi sumber daya untuk memastikan hubungan antara kebutuhan sumber daya dan kendala sumber daya sehingga tujuan manajemen dapat dicapai. Berikut ini adalah beberapa metode dan kebijakan umum untuk konfigurasi sumber daya dalam manajemen proyek.

(1) Metode alokasi sumber daya:

- Metode jalur kritis (CPM) membagi sebuah proyek menjadi beberapa tugas terpisah dan menentukan durasi setiap tugas setelah menghubungkan tugas-tugas ini secara logis. Jalur kritis adalah jalur tugas yang terbentuk dengan durasi terpanjang. Metode jalur kritis adalah cara terbaik untuk memprioritaskan sumber daya yang penting dalam manajemen proyek. Metode ini tidak hanya dapat mengalokasikan sumber daya secara optimal, tetapi juga dapat memperpendek periode konstruksi secara keseluruhan dan mengurangi biaya yang tidak diperlukan. Oleh karena itu, ini juga merupakan cara yang murah untuk mengalokasikan sumber daya.
- Metode Rantai Kritis: Metode rantai kritis adalah perluasan dari metode kritis. Namun, metode rantai kritis mempertimbangkan sumber daya bottleneck terlebih dahulu,

menyeimbangkan sumber daya bottleneck, dan kemudian mengambil rute tugas terpanjang yang terbentuk sebagai rantai kritis. Dalam metode rantai kritis, jumlah tugas yang membatasi penyelesaian proyek dianggap sebagai rantai kritis. Metode rantai kritis mengutamakan waktu dan sumber daya yang dibatasi untuk proyek. Di satu sisi, manajemen waktu kerja secara keseluruhan dapat mengurangi dampak pada jadwal proyek; di sisi lain, konflik sumber daya dan persaingan sumber daya antar tugas dapat dipertimbangkan untuk mengelola jadwal proyek dengan memonitor dan mengatur buffer. Pendekatan jalur kritis menganalisis durasi maksimum proyek tanpa mempertimbangkan kendala sumber daya; aturan rantai kritis menyatakan bahwa kendala sumber daya Oleh karena itu, metode rantai kritis dapat digunakan untuk menggantikan metode jalur kritis jika kendala proyek dipertimbangkan.

- Metode keseimbangan sumber daya: Salah satu metode yang paling banyak digunakan saat ini adalah metode keseimbangan sumber daya. Metode ini mengurangi fluktuasi jumlah sumber daya yang diperlukan untuk proyek dan memungkinkan penggunaan sumber daya yang seimbang dan efisien oleh berbagai tugas yang dilakukan proyek. Metode keseimbangan sumber daya terdiri dari dua metode: metode grafis dan metode penilaian formula. Metode grafis menunjukkan dan menganalisis penggunaan dan alokasi sumber daya untuk setiap tugas dalam proyek; metode ini dapat menunjukkan alokasi sumber daya secara intuitif. Metode penilaian formula melakukan perhitungan untuk menilai apakah alokasi sumber daya untuk setiap tugas dalam proyek berkembang secara menguntungkan. Dengan menggunakan metode ini, penilaian dapat menjadi lebih ilmiah dan akurat. Meskipun kedua pendekatan ini tidak cocok untuk operasi tertentu, keduanya dapat mencapai tujuan untuk mendorong alokasi sumber daya yang seimbang.

(2) Strategi alokasi sumber daya

Alokasi sumber daya dalam manajemen proyek membutuhkan strategi konfigurasi dan metode yang baik.

Memprioritaskan tugas-tugas proyek: Selama proses manajemen proyek, setiap tugas memiliki tujuan yang ingin dicapai, tetapi tujuan-tujuan ini tidak selalu harus diprioritaskan secara bersamaan. Unit manajemen proyek biasanya menentukan tugas mana yang harus diprioritaskan dalam manajemen proyek yang sebenarnya berdasarkan nilai dan kemampuan mereka. Prioritas tugas juga harus disesuaikan sesuai dengan durasi dan kemajuan proyek. Hanya dengan cara ini kebutuhan proyek yang sebenarnya dapat digambarkan dengan lebih jelas. Agar alokasi sumber daya lebih ilmiah dan masuk akal, prioritaskan tugas-tugas penting.

Menentukan jenis dan jumlah sumber daya yang diperlukan untuk setiap tugas dalam proyek: Pendekatan Work Breakdown Structure (WBS) dapat digunakan oleh organisasi manajemen proyek untuk menentukan jenis dan jumlah sumber daya yang diperlukan untuk setiap tugas dalam proyek, membuat anggaran berdasarkan hal ini, mengalokasikan anggaran untuk setiap tugas berdasarkan waktu, dan jika diperlukan, melakukan penyesuaian. Tidak hanya persyaratan kualitas sumber daya yang tinggi untuk proyek, tetapi juga batas waktu untuk alokasi sumber daya juga harus dipertimbangkan dalam manajemen proyek. Ini berarti bahwa persyaratan sumber daya harus ditentukan setiap langkah dalam proses alokasi sumber daya agar sumber daya dapat dialokasikan secara efektif dan tepat waktu. Perlu diingat bahwa dalam proses manajemen multi-proyek, ada juga masalah seperti modal, pasar, dan personel, yang membutuhkan alokasi sumber daya yang terbatas.

Menganalisis keterbatasan sumber daya: Saat memulai sebuah proyek, ada kemungkinan bahwa ada sumber daya yang terbatas. Jika tidak ada sumber daya yang cukup, jadwal proyek biasanya akan tertunda, dan dalam kasus yang lebih serius, proyek bahkan akan gagal. Oleh karena itu, analisis masalah kekurangan sumber daya harus dilakukan terlebih dahulu; ini dikenal sebagai analisis kendala sumber daya. Analisis kendala sumber daya dapat mencegah kelangkaan sumber daya dan memastikan bahwa semua tugas proyek selesai dengan cepat. Ketika analisis kendala sumber daya tidak dilakukan dalam batas waktu, ketika sumber daya yang digunakan untuk proyek sekali pakai Manajer proyek biasanya meningkatkan investasi jika dana tidak mencukupi. Namun, investasi tidak dapat ditingkatkan tanpa meningkatkan proyek apa pun. Oleh karena itu, selama alokasi sumber daya, analisis kendala sumber daya harus dilakukan untuk memastikan bahwa sumber daya digunakan dengan cara yang masuk akal.

Pengurutan Tugas: Proyek besar akan dibagi menjadi beberapa tugas selama proses manajemen proyek, yang melibatkan penjadwalan dan pembagian tugas. Pengaturan jadwal dan alokasi tugas biasanya membutuhkan metode tertentu; salah satu metode ini adalah teknologi perencanaan jaringan yang umum digunakan. Teknik perencanaan jaringan adalah teknologi manajemen yang digunakan untuk perencanaan dan pengendalian proyek. Ini memungkinkan Anda membuat diagram jaringan yang mudah dipahami dan menunjukkan titik waktu proyek, konsumsi sumber daya, dan sistem informasi lainnya. Selain itu, mereka dapat menunjukkan hubungan logis antara setiap tugas dan batasan waktu mereka. Diagram jaringan adalah model grafis dari teknologi perencanaan jaringan dan keseluruhan organik yang lebih luas. Pemetaan jaringan adalah komponen utama dari metode perencanaan jaringan.

Menghitung parameter waktu diagram jaringan adalah cara untuk menentukan jalur kritis. Setelah menentukan jalur kritis, rencana awal rencana jaringan ditingkatkan, dan skema manajemen proyek yang ideal dicari di bawah batasan tertentu. Seberapa cepat tugas-tugas ini diselesaikan secara langsung berdampak pada lamanya proyek secara keseluruhan. Bagan Gantt adalah metode umum lainnya untuk pengurutan tugas yang sederhana dan praktis. Ini menggunakan sumbu horizontal untuk menunjukkan waktu, sumbu vertikal untuk menunjukkan tugas, dan diagram batang untuk menunjukkan waktu mulai, durasi, dan penyelesaian tugas, serta informasi tentang kemajuan. Gantt chart dapat secara langsung menunjukkan tugas yang belum selesai dan membantu menilai apakah kemajuan dalam suatu tugas memenuhi kemajuan yang diharapkan.

(3) Model alokasi sumber daya multi-proyek

Jika organisasi akan menjalankan beberapa proyek pada saat yang sama, untuk membuat tingkat pemanfaatan sumber daya tertinggi dan total durasi terpendek, maka diperlukan model alokasi sumber daya multi proyek, dan metode spesifiknya adalah: Perkiraan durasi dan identifikasi sumber daya, yaitu dalam menentukan durasi setiap proyek dan sumber daya yang dibutuhkan untuk mengidentifikasi setiap proyek, atas dasar menggambar setiap diagram jaringan proyek, dan menemukan adanya hubungan persaingan sumber daya proyek; Pengaturan prioritas adalah menetapkan prioritas setiap proyek, sehingga dapat mencapai tujuan alokasi sumber daya multi proyek dengan memenuhi kebutuhan sumber daya proyek dengan prioritas tinggi. Identifikasi rantai kunci dan atur penyangga, yaitu mencari tahu rantai kunci dengan menganalisis kendala sumber daya, dan mengatur penyangga untuk meningkatkan pemanfaatan sumber daya; Meningkatkan teknologi dan kontrol jadwal, yaitu menemukan masalah yang ada dalam alokasi sumber daya, perencanaan jadwal dan pengoptimalan durasi manajemen multi-proyek, dan melakukan perbaikan berkelanjutan. Model konfigurasi sumber daya untuk berbagai proyek.

3.3 Organisasi Manajemen Keamanan E-commerce

Organisasi yang menangani keamanan bisnis e-commerce semakin penting. Apakah undang-undang dan peraturan diterapkan secara efektif, apakah struktur organisasi manajemen keamanan e-commerce masuk akal, apakah tugasnya sesuai, dan apakah implementasi peraturan berdampak langsung pada kinerja manajemen keamanan e-commerce? Dianalisis bagaimana organisasi manajemen keamanan e-niaga didirikan, bagaimana organisasi tersebut berjalan, dan bagaimana organisasi tersebut berkembang seiring berjalannya waktu.

3.3.1 Pembentukan Organisasi Manajemen Keamanan E-Commerce

1. Persyaratan dasar organisasi manajemen keamanan

Persyaratan dasar organisasi manajemen keamanan Manajemen keselamatan adalah perilaku yang terencana dan terorganisir, dan pencapaian tujuan manajemen keselamatan bergantung pada organisasi manajemen keselamatan yang tepat dan alokasi sumber daya yang tepat. Organisasi manajemen keselamatan harus dianggap sebagai sistem terintegrasi yang memiliki perintah bebas dari atas ke bawah. Ini memungkinkan manajemen keamanan perusahaan e-niaga untuk mencapai manajemen berlapis-lapis, terpusat. Organisasi yang bertanggung jawab untuk mengelola keamanan perdagangan elektronik harus memenuhi persyaratan berikut.

Ada desain struktur yang logis. Didasarkan pada pembagian fungsi manajemen dan penentuan tanggung jawab, kekuasaan, dan struktur internal organisasi untuk manajemen keamanan e-commerce, konsep desain struktur digunakan dalam perusahaan e-commerce. Pada saat yang sama, departemen harus dibentuk secara wajar secara horizontal dan hierarki wajar harus dibagi secara vertikal. Ini akan membentuk garis horizontal ke tepi dan garis vertikal ke ujung sistem organisasi manajemen keamanan perdagangan elektronik.

Wewenang dan tanggung jawab ditetapkan dengan jelas. Untuk menghindari konflik kepentingan di antara departemen dan tingkat dalam organisasi manajemen keamanan e-commerce, penting untuk menjelaskan tanggung jawab dan wewenang masing-masing departemen dan tingkat agar jelas tentang apa yang harus dilakukan. Jumlah karyawan yang memadai Untuk memenuhi kebutuhan pengembangan yang sebenarnya, organisasi manajemen keamanan e-commerce harus memiliki staf yang memadai yang memiliki tanggung jawab di berbagai departemen dan tingkat. Orang-orang, terutama administrator dan teknisi keamanan, harus memiliki pengetahuan dan keterampilan profesional.

Untuk memastikan bahwa setiap pekerjaan aman dan efektif, organisasi manajemen keselamatan perdagangan elektronik membuat dan menerapkan peraturan dan regulasi. Organisasi manajemen keamanan perdagangan elektronik harus menetapkan metode yang efektif untuk berkomunikasi dengan orang-orang dalam organisasi mereka sehingga informasi dapat dikomunikasikan dengan mudah.

Pastikan komunikasi dengan dunia luar. Organisasi manajemen keamanan e-commerce tidak hanya harus memastikan bahwa semua informasi dikomunikasikan dengan baik di antara departemen internal mereka, tetapi juga harus memastikan bahwa mereka berkomunikasi dengan orang-orang dan lembaga di luar negeri untuk mendapatkan bimbingan dan pengawasan dari departemen pemerintah terkait.

2. Faktor-faktor yang mempengaruhi pembentukan organisasi manajemen keamanan e-commerce

(1) Tujuan strategis manajemen keamanan e-commerce

Organisasi manajemen keamanan perdagangan elektronik adalah jaminan penting untuk mencapai tujuan strategis manajemen keamanan perdagangan elektronik. Tujuan strategis manajemen keamanan perdagangan elektronik harus menentukan struktur organisasi manajemen keamanan perdagangan elektronik. Untuk tujuan strategis manajemen keamanan e-commerce yang sederhana, organisasi manajemen keamanan e-commerce dapat menggunakan struktur organisasi organik. Struktur organisasi organik longgar, fleksibel, fleksibel, kompleksitas rendah, regularisasi rendah, dan desentralisasi. Namun, untuk tujuan manajemen keamanan e-commerce yang kompleks, struktur organisasi mekanis dapat digunakan, yang stabil, kaku, dan memiliki banyak fitur yang unik.

(2) Tingkat organisasi manajemen keamanan perdagangan

Elektronik ditentukan oleh ukuran perusahaan perdagangan elektronik dan sumber daya yang tersedia. Misalnya, perusahaan besar akan membentuk organisasi manajemen keamanan e-commerce yang lengkap untuk mengelola keamanan e-commerce. Organisasi ini akan terdiri dari kepala petugas keamanan, direktur, administrator, dan teknisi keamanan. Secara umum, organisasi manajemen keamanan e-niaga lebih besar jika perusahaan lebih besar; bisnis e-niaga kecil biasanya hanya memiliki satu administrator keamanan atau bahkan tidak memiliki organisasi manajemen keamanan e-niaga yang lengkap Personel, seperti administrator sistem atau administrator jaringan, melakukan tugas yang sama pada waktu yang sama.

(3) Persyaratan bisnis dan keamanan perusahaan e-commerce

Persyaratan bisnis dan keamanan perusahaan e-commerce juga akan mempengaruhi pembentukan organisasi manajemen keamanan e-commerce. Jika perusahaan e-commerce menggunakan pihak ketiga pembayaran, keuangan jaringan, dan bisnis lain dengan persyaratan keamanan yang tinggi, mereka akan sangat mementingkan manajemen keamanan dan kemudian membentuk organisasi manajemen keamanan yang hampir sempurna

(4) Budaya keamanan e-commerce

Istilah "budaya keamanan e-commerce" mengacu pada jumlah nilai keselamatan atau gagasan keselamatan yang secara bertahap dibentuk oleh perusahaan e-commerce selama waktu yang lama, atribut keselamatan yang ditunjukkan oleh perilaku profesional karyawan, dan lingkungan keselamatan perusahaan. Perusahaan e-commerce dengan budaya keselamatan tingkat tinggi akan lebih memperhatikan pembangunan organisasi manajemen keamanan perdagangan elektronik.

3. Struktur dan fungsi manajemen keamanan e-commerce

(1) Struktur organisasi dan fungsi manajemen keamanan perusahaan perdagangan elektronik yang besar

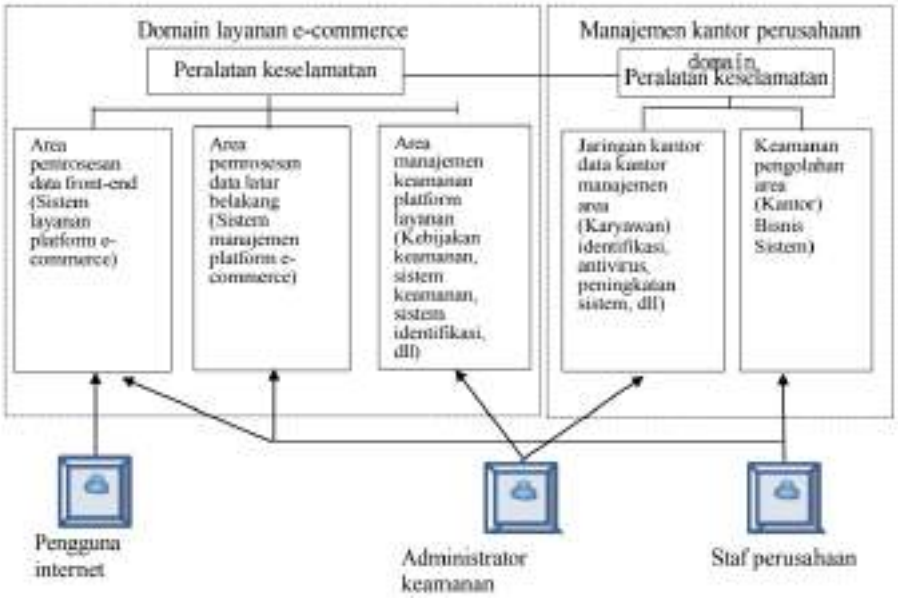
Perusahaan e-commerce besar biasanya mengacu pada perusahaan platform e-commerce besar. Perusahaan platform e-commerce menyediakan platform di mana pedagang dan konsumen dapat berdagang secara online dan menjamin perdagangan yang lancar. Pedagang juga dapat memanfaatkan infrastruktur jaringan, platform pembayaran, dan platform manajemen yang disediakan oleh perusahaan platform e-commerce untuk menjalankan aktivitas bisnis mereka. Contoh struktur organisasi untuk manajemen keamanan e-commerce Komite manajemen keamanan. Komite ini juga bertanggung jawab untuk mengambil keputusan tentang urusan manajemen keamanan utama. Beberapa direktur dewan direksi dan kepala petugas keamanan adalah anggota utamanya. Selain tanggung jawab lainnya, CEO bertanggung jawab penuh atas manajemen keamanan harian dan melaporkan insiden keamanan penting kepada komite manajemen keamanan.

Untuk perusahaan e-commerce yang besar, posisi departemen teknologi informasi sangat penting. Departemen teknologi informasi biasanya terdiri dari departemen data, departemen operasi dan pemeliharaan, departemen penelitian dan pengembangan, dan departemen keamanan informasi. Departemen keamanan informasi dapat membentuk departemen keamanan serangan dan pertahanan dan departemen keamanan bisnis, yang masing-masing berfokus pada serangan dan pertahanan. Keamanan web, keamanan aplikasi, solusi keamanan produknya sendiri, dan praktik siklus hidup pengembangan yang aman (SDL) adalah semua tanggung jawab kelompok keamanan aplikasi. Kelompok keamanan arsitektur menangani keamanan sistem informasi, keamanan jaringan, konstruksi sistem keamanan, dan tugas lainnya. Kelompok produk keamanan secara independen mengembangkan alat keamanan. Pengendalian risiko keamanan layanan adalah fokus utama departemen keamanan layanan. Biasanya, tim-tim berikut dibentuk: Tim keamanan akun bertanggung jawab atas pengendalian risiko akun, seperti anti-pemindaian nomor, anti-tabrakan basis data, dll. Grup Produk Pengendalian Risiko bertanggung jawab atas pengendalian risiko bisnis, seperti anti-penipuan, keamanan transaksi, dll. Selain departemen teknologi informasi, departemen sumber daya manusia, departemen keuangan, dan departemen administrasi juga berpartisipasi dalam departemen manajemen keamanan perusahaan, dan masing-masing memikul tanggung jawab yang sesuai terkait keamanan. Misalnya, departemen sumber daya manusia bertanggung jawab atas perekrutan dan pemecatan personel, masalah pendidikan keselamatan, pelatihan karyawan, dll. Salah satu departemen di perusahaan adalah departemen hukum, yang bertanggung jawab

untuk memastikan bahwa operasi dan kebijakan perusahaan sesuai dengan peraturan dan hukum yang ada. Departemen audit juga bertanggung jawab untuk menstandarisasi akuntansi keuangan perusahaan dan mendorong operasi yang sah dan patuh. Meskipun departemen pemasaran dan penjualan tidak langsung terlibat dalam manajemen keamanan perusahaan, izin latar belakang mereka juga dapat menyebabkan beberapa masalah keamanan, yang berarti mereka juga harus memenuhi tanggung jawab keamanan yang sesuai struktur dan fungsi organisasi manajemen keamanan perusahaan e-commerce kecil dan menengah: Struktur dan fungsi organisasi manajemen keamanan perusahaan e-commerce kecil dan menengah sangat terkait dengan struktur aplikasi keamanan informasi dan mode konstruksi sistem keamanan informasi.

(2) Selain departemen teknologi informasi, departemen sumber daya manusia, departemen keuangan, dan departemen administrasi juga berpartisipasi dalam departemen manajemen keamanan perusahaan, dan masing-masing memikul tanggung jawab yang sesuai terkait keamanan. Misalnya, departemen sumber daya manusia bertanggung jawab atas perekrutan dan pemecatan personel, masalah pendidikan keselamatan, pelatihan karyawan, dll. Salah satu departemen di perusahaan adalah departemen hukum, yang bertanggung jawab untuk memastikan bahwa operasi dan kebijakan perusahaan sesuai dengan peraturan dan hukum yang ada. Departemen audit juga bertanggung jawab untuk menstandarisasi akuntansi keuangan perusahaan dan mendorong operasi yang sah dan patuh. Meskipun departemen pemasaran dan penjualan tidak langsung terlibat dalam manajemen keamanan perusahaan, izin latar belakang mereka juga dapat menyebabkan beberapa masalah keamanan, yang berarti mereka juga harus memenuhi tanggung jawab keamanan yang sesuai struktur dan fungsi organisasi manajemen keamanan perusahaan e-commerce kecil dan menengah: Struktur dan fungsi organisasi manajemen keamanan perusahaan e-commerce kecil dan menengah sangat terkait dengan struktur aplikasi keamanan informasi dan mode konstruksi sistem keamanan informasi. Struktur aplikasi keamanan informasi perusahaan e-commerce kecil dan menengah digambarkan dalam Gambar 3.1.

Bisnis e-commerce kecil dan menengah beroperasi di domain layanan e-commerce, yang mencakup area pemrosesan data front-end, area pemrosesan data back-end, dan area manajemen keamanan platform layanan. Area pemrosesan data front-end, yaitu sistem layanan platform e-commerce, termasuk sistem aplikasi e-commerce dan basis datanya, berfungsi sebagai area di mana pelanggan berinteraksi dengan platform e-commerce melalui Internet.



Gambar 3.1 Struktur aplikasi keamanan informasi perusahaan *e-commerce* kecil dan menengah

Area pemrosesan data back-end mencakup berbagai sistem manajemen platform e-commerce, serta basis datanya, seperti sistem manajemen pengguna dan komoditas, yang dapat diakses oleh karyawan. Zona manajemen keamanan platform layanan terdiri dari kebijakan keamanan, sistem keamanan, dan sistem otentikasi identitas. Administrator keamanan bertugas mengelola sumber daya terpadu, manajemen hak pengguna, dan manajemen otentikasi untuk memastikan bahwa platform layanan e-commerce beroperasi dengan aman. Zona manajemen keamanan platform layanan hanya dapat diakses oleh administrator keamanan.

Perusahaan e-commerce kecil dan menengah menggunakan istilah "domain manajemen kantor" untuk menggambarkan wilayah di mana operasi dan proses bisnis internal dilakukan. Ini termasuk area pemrosesan data kantor dan area manajemen keamanan jaringan kantor. Area pemrosesan data kantor terdiri dari sistem bisnis kantor, seperti berbagi file, sistem personalia, sistem keuangan, dan database lainnya. Area ini tertutup untuk publik dan hanya diizinkan untuk diakses oleh karyawan. Kebijakan kontrol akses dan perangkat keamanan informasi dapat digunakan untuk mencegah akses yang tidak sah antara domain layanan e-commerce dan domain manajemen kantor perusahaan.

Cara perusahaan e-commerce kecil dan menengah membangun sistem keamanan informasi: Dalam struktur aplikasi keamanan informasi mereka, perusahaan biasanya membangun domain manajemen kantor perusahaan sendiri. Ini berarti bahwa perusahaan membangun dan memelihara sistem keamanan informasi di wilayah tersebut dan bertanggung jawab atas semua tugas yang berkaitan dengan manajemen risiko sistem keamanan informasi. Ada tiga cara berbeda untuk membangun sistem keamanan informasi domain layanan e-

commerce, tergantung pada skala dan kebutuhan bisnis perusahaan: membuat sendiri, menyewa sumber daya, atau menyewa toko. Perlu diingat bahwa perusahaan e-commerce kecil dan menengah memiliki tanggung jawab manajemen risiko yang berbeda untuk sistem keamanan informasi mereka, yang mencakup keamanan fisik, keamanan host, keamanan jaringan, keamanan aplikasi, dan keamanan data.

- Model Membangun Sendiri: Perusahaan e-commerce kecil dan menengah menggunakan mode membangun sendiri karena mereka bergantung pada layanan akses Internet yang disediakan oleh operator telekomunikasi. Perusahaan-perusahaan ini membangun dan memelihara platform e-commerce yang menyediakan layanan transaksi eksternal, yang mencakup infrastruktur fisik, host, layanan jaringan, dan keamanan sistem informasi yang sesuai. Perusahaan-perusahaan ini akan memikul semua tanggung jawab manajemen risiko untuk keseluruhan platform e-commerce.
- Mode penyewaan sumber daya: Ada tiga mode penyewaan sumber daya: penyewaan sumber daya fisik, penyewaan sumber daya fisik dan host, dan penyewaan sumber daya fisik, host, dan layanan jaringan. Dalam mode penyewaan sumber daya fisik, perusahaan e-commerce kecil dan menengah mengandalkan infrastruktur fisik yang disediakan oleh penyedia layanan seperti operator telekomunikasi dan pusat data Internet untuk membangun platform ecommerce. Perusahaan e-commerce kecil dan menengah memikul tanggung jawab manajemen risiko keamanan host, keamanan jaringan, dan keamanan data dasar, dan penyedia layanan sumber daya memikul tanggung jawab manajemen risiko keamanan fisik. Dalam mode menyewa sumber daya fisik dan host, perusahaan e-commerce kecil dan menengah mengandalkan infrastruktur fisik yang disediakan oleh penyedia layanan sumber daya, seperti operator telekomunikasi dan pusat data Internet, dan menyewa host yang disediakan oleh penyedia layanan sumber daya untuk membangun platform layanan e-commerce. Penyedia layanan sumber daya memikul tanggung jawab kalender risiko keamanan fisik dan keamanan host, dan perusahaan e-niaga kecil dan menengah tanggung jawab manajemen risiko keamanan jaringan, keamanan aplikasi, dan keamanan data. Dalam mode penyewaan sumber daya layanan fisik, host, dan jaringan, perusahaan e-niaga kecil dan menengah mengandalkan infrastruktur fisik yang disediakan oleh penyedia layanan sumber daya seperti operator telekomunikasi dan pusat data Internet, dan menyewa host sistem dan sumber daya layanan jaringan yang disediakan oleh penyedia layanan sumber daya untuk membangun platform e-niaga. Penyedia layanan sumber daya memikul tanggung jawab manajemen risiko keamanan fisik, keamanan host, keamanan

jaringan, dan keamanan data dasar, dan perusahaan e-niaga kecil dan menengah memikul tanggung jawab manajemen risiko keamanan aplikasi dan keamanan data parsial.

- Mode penyewaan toko: Mode penyewaan toko mengacu pada mode di mana perusahaan e-niaga kecil dan menengah menyewa sumber daya toko online yang disediakan oleh platform e-niaga pihak ketiga untuk menyediakan layanan e-niaga bagi konsumen. Perusahaan e-niaga kecil dan menengah hanya memikul tanggung jawab manajemen risiko keamanan jaringan dalam domain manajemen kantor, sementara penyedia layanan sumber daya memikul tanggung jawab manajemen risiko keamanan fisik, keamanan host, keamanan aplikasi, dan keamanan data. Artinya, sistem keamanan informasi perusahaan e-niaga kecil dan menengah yang menggunakan mode persewaan toko disediakan oleh platform e-niaga pihak ketiga, dan perusahaan menyediakan layanan e-niaga untuk konsumen melalui platform e-niaga pihak ketiga.

Struktur organisasi keamanan perusahaan e-commerce kecil dan menengah: Karena mode konstruksi sistem keamanan informasi yang berbeda, perusahaan e-commerce kecil dan menengah memiliki struktur organisasi manajemen keamanan yang berbeda.

Struktur organisasi manajemen keamanan yang dibangun sendiri: Jika perusahaan e-commerce kecil dan menengah menggunakan sistem keamanan informasi yang dibangun sendiri, mereka Struktur organisasi manajemen keamanan dapat mengacu pada struktur organisasi manajemen keamanan perusahaan e-commerce besar.

Struktur organisasi manajemen keamanan mode penyewaan sumber daya: Jika perusahaan e-niaga kecil dan menengah mengadopsi mode penyewaan sumber daya untuk membangun sistem keamanan informasi, perusahaan tidak hanya bertanggung jawab atas pembangunan jaringan dan manajemen keamanan dalam domain manajemen kantor perusahaan, tetapi juga melakukan pembangunan sumber daya informasi dan manajemen keamanan tertentu.

3.3.2 Pengoperasian Organisasi Manajemen Keamanan E-commerce

Berikut ini terutama membahas bagaimana organisasi manajemen keamanan e-commerce beroperasi dari dua aspek: mekanisme operasi dan jaminan operasi.

1. Mekanisme operasi organisasi manajemen keamanan e-commerce

Pertama, mekanisme motivasi operasi organisasi manajemen keamanan e-commerce adalah dasar dari penerapan strategi keamanan perusahaan e-commerce. Organisasi manajemen keamanan e-commerce bekerja untuk strategi keamanan perusahaan e-commerce dengan tujuan meminimalkan investasi untuk mencapai manfaat keamanan maksimal.

Kedua, sistem untuk membuat keputusan tentang operasi organisasi. Dalam manajemen keselamatan, para pemimpin organisasi manajemen keselamatan e-commerce, termasuk manajer senior dan komite manajemen keselamatan, memiliki otoritas tertinggi untuk membuat keputusan. Mereka bertanggung jawab untuk memulai proses manajemen keselamatan, memastikan manajemen keselamatan dan peran yang diberikan kepada manajemen keselamatan. Mereka juga bertanggung jawab untuk melindungi aset informasi. Mereka juga bertanggung jawab untuk memastikan bahwa fasilitas pemrosesan data dan sumber daya yang terkait dengan otorisasi memenuhi aliran operasi manajemen otorisasi. Mereka juga bertanggung jawab untuk memberikan komitmen yang sesuai dan menyediakan sumber daya yang cukup untuk mendorong karir karyawan.

Ketiga, sistem informasi yang digunakan dalam operasi perusahaan yang menangani keamanan perdagangan elektronik. Informasi sangat penting untuk pengambilan keputusan, dan organisasi manajemen keamanan perdagangan elektronik harus membuat mekanisme informasi yang sensitif dan efisien, serta metode dan saluran untuk pengumpulan, pengiriman, pemrosesan, penyimpanan, pengambilan, dan analisis informasi. Organisasi juga harus memberi para pengambil keputusan saran dari para ahli keamanan. Selain itu, penting untuk menjaga komunikasi yang konsisten dengan otoritas penegak hukum, pihak yang berwenang, penyedia layanan, dan lainnya

Keempat, tanggung jawab sosial dalam menjalankan operasi organisasi manajemen keselamatan e-commerce. Perusahaan e-commerce berada di lingkungan sosial tertentu, melakukan fungsi sosial tertentu, dan merupakan jenis organisasi sosial. Karena itu, perusahaan manajemen keselamatannya juga harus melakukan tanggung jawab sosial tertentu saat menjalankan bisnisnya.

2. Jaminan operasi organisasi manajemen keamanan e-commerce

Operasi organisasi ini secara langsung memengaruhi pencapaian tujuan manajemen keamanan e-commerce, sehingga proses operasinya memerlukan perlindungan dari peraturan dan regulasi yang sesuai, perlindungan investasi sumber daya, perlindungan penilaian kinerja, dan perlindungan budaya keselamatan.

Pertama, keamanan hukum. Sangat penting bagi organisasi manajemen keamanan e-commerce untuk membuat dan menerapkan aturan dan regulasi. Aturan dan regulasi harus mencakup struktur organisasi, tanggung jawab, prosedur operasi, personel, norma operasi, dan pembagian hak pengambilan keputusan. Perumusan dan pelaksanaan undang-undang adalah proses pengumpulan dan pengembangan yang berkelanjutan.

Kedua, harus ada jaminan tentang jumlah sumber daya yang dibutuhkan untuk menjalankan organisasi manajemen keamanan perdagangan elektronik. Hanya dengan jumlah sumber daya yang cukup, akan mungkin untuk memastikan bahwa pengembangan organisasi akan berjalan lancar. Dengan jumlah sumber daya yang cukup, akan mungkin untuk menyediakan tenaga kerja, sumber daya material, dan sumber daya keuangan yang cukup.

Ketiga, garansi untuk penilaian kinerja. Salah satu jaminan penting untuk pengoperasian organisasi manajemen keamanan e-commerce adalah pembentukan penilaian kinerja yang wajar dan sempurna dengan indikator penilaian yang rinci, jelas, dan masuk akal untuk memandu perilaku personel terkait. Penilaian kinerja adalah semacam mekanisme pengawasan, dan hanya melalui mekanisme ini organisasi manajemen keamanan e-commerce dapat melacak, mencatat, dan mengevaluasi kemampuan personel terkait untuk memenuhi tujuan.

Keempat, keamanan budaya. Konsep keselamatan manajemen dan perilaku keselamatan setiap anggota membentuk budaya keselamatan organisasi manajemen keselamatan perdagangan elektronik. Dengan koreksi otomatis, organisasi manajemen keselamatan perdagangan elektronik dapat menahan diri dan beroperasi dengan lancar.

3.3.3 Perubahan Struktur Manajemen Keamanan Perdagangan Elektronik

Organisasi manajemen keamanan perdagangan elektronik adalah entitas yang terdiri dari banyak komponen. Reformasi diperlukan saat komponen internalnya dan lingkungan luarnya berubah. Reformasi organisasi manajemen keamanan e-niaga berarti manajer mengambil tindakan untuk mengubah struktur, sistem, anggota, budaya, perilaku, dll. organisasi asli untuk menyesuaikan diri dengan perubahan eksternal dan meningkatkan kinerja organisasi. Tujuan pengembangan manajemen keamanan e-commerce biasanya terkait dengan perubahan organisasinya. Organisasi manajemen keamanan e-commerce harus melakukan reformasi struktur organisasi, membangun dan meningkatkan mekanisme operasi organisasi untuk meningkatkan fleksibilitas dan kemampuan untuk menyesuaikan diri dengan lingkungan eksternal. Selain itu, Anda harus mendorong inovasi dan terus meningkatkan pengetahuan, keterampilan, perilaku, dan kesadaran manajemen keselamatan organisasi untuk meningkatkan keamanan organisasi.

1. Tren reformasi organisasi manajemen keamanan e-commerce

Reformasi organisasi manajemen keamanan e-commerce telah menyebabkan penurunan hierarki, jaringan, dan struktur organisasi yang rata. Beberapa elemen berikut terutama menunjukkan penurunan hierarki organisasi.

Yang pertama adalah komunikasi vertikal yang lebih baik, yang berarti lebih sedikit perbedaan status antara tingkat organisasi yang berbeda, kurangnya keyakinan tentang hierarki, dan lebih banyak pertukaran horizontal.

Yang kedua adalah peningkatan pertukaran horizontal. Jumlah karyawan yang bekerja pada tingkat organisasi yang sama yang bekerja pada fungsi yang berbeda semakin meningkat, yang menyebabkan mereka menjadi generalis. Sebagai contoh, teknisi keamanan di perusahaan e-commerce kecil biasanya bekerja sebagai administrator paruh waktu.

Ketiga, penguatan manajemen berbasis manusia. Organisasi memberikan wewenang penuh kepada karyawan atau departemen untuk menjadi lebih mandiri dan bebas. Organisasi hirarkis tradisional memiliki banyak manajemen menengah, yang menyebabkan mereka bersifat mekanis, kaku, dan tidak efektif. Perataan dapat meningkatkan efisiensi dan mengurangi biaya manajemen dengan memperpendek rantai komando, mempercepat transmisi informasi, dan meningkatkan cara komunikasi.

Dengan menggunakan jaringan komputer secara luas, organisasi dapat memodernisasi proses pengumpulan, pengumpulan, transmisi, dan kontrol informasi. Selain itu, jaringan komputer mendorong pergeseran struktur organisasi dari hierarki birokrasi ke hierarki datar. Dalam struktur pembedahan, struktur tim dianggap sebagai struktur prosedural. Staf organisasi dapat melampaui batas departemen asli dan menuju ke tujuan manajemen keamanan organisasi secara keseluruhan, membentuk tim atau kelompok yang sebanding, mandiri, dan inovatif.

2. Faktor yang menyebabkan perubahan organisasi dalam manajemen keamanan e-commerce

Organisasi manajemen keamanan e-commerce berkembang seiring berjalannya waktu, dipengaruhi oleh tekanan internal dan eksternal. Beberapa contoh tekanan ini termasuk jumlah bisnis yang terbatas, koordinasi yang tidak efektif, tanggung jawab yang tidak jelas, uang yang hilang, perlambatan, dan fenomena yang tidak dapat diprediksi lainnya. Semua ini dapat menghambat pencapaian tujuan manajemen keamanan e-commerce Oleh karena itu, reformasi organisasi manajemen keamanan e-commerce sangat penting untuk kemajuan e-commerce. Faktor-faktor yang mendorong reformasi terutama terdiri dari faktor eksternal dan internal. Faktor eksternal terutama mendorong perubahan organisasi, seperti kemajuan teknologi informasi, peraturan dan undang-undang yang relevan, perkembangan ekonomi domestik dan internasional, dan keamanan jaringan. Faktor internal terutama mendorong perubahan organisasi, seperti sistem manajemen, tanggung jawab Fenomena pelimpahan uang di antara

karyawan menunjukkan bahwa struktur organisasi sangat membutuhkan reformasi jika wewenang dan tanggung jawab manajemen tidak jelas.

3. Faktor-faktor yang mempengaruhi reformasi struktur organisasi manajemen keamanan e-commerce

Faktor-faktor seperti faktor lingkungan, faktor strategis, faktor skala, dan lainnya sangat memengaruhi reformasi struktur organisasi manajemen keamanan e-commerce. Secara umum, lingkungan terdiri dari lingkungan umum dan lingkungan khusus. Lingkungan umum mencakup faktor politik, ekonomi, budaya, ilmu pengetahuan, dan teknologi yang berdampak langsung dan tidak langsung pada organisasi. Lingkungan khusus mencakup faktor seperti pesaing, mitra, dan komposisi organisasi, yang unik untuk setiap organisasi dan akan berubah seiring dengan perkembangan lingkungan umum. Struktur organisasi hanya dapat berfungsi dengan baik jika disesuaikan dengan perubahan lingkungan yang terus-menerus. Oleh karena itu, manajer harus terus mengubah struktur organisasi untuk menyesuaikannya dengan lingkungan.

Di sini, fokus utama adalah pada strategi manajemen keamanan e-commerce. Strategi ini berbicara tentang tujuan keseluruhan untuk menentukan dan memengaruhi sifat dan tujuan organisasi manajemen keamanan perdagangan elektronik, serta langkah-langkah dan metode untuk mencapai tujuan tersebut. Strategi ini juga menentukan struktur organisasi dan langkah-langkah yang akan diambil untuk mencapainya. Untuk mengimplementasikan strategi manajemen keamanan e-bisnis secara efektif, struktur organisasi harus disesuaikan dengan strategi tersebut. Faktor-faktor strategis mengharuskan manajer untuk memikirkan strategi pengembangan organisasi dari sudut pandang struktur organisasi yang ada, tetapi mereka harus membuat strategi baru untuk menyesuaikan struktur organisasi yang ada dengan perubahan yang terjadi di luar.

Salah satu faktor penting yang mempengaruhi struktur organisasi adalah ukurannya; ukuran yang lebih besar akan menyebabkan organisasi lebih kompleks, lebih standarisasi, dan lebih spesialisasi. Ini karena ketika bisnis suatu organisasi berkembang, jumlah karyawan meningkat, dan tingkat lapisan manajemen meningkat, pembagian spesialisasi menjadi semakin rumit.

4. Proses reformasi struktur organisasi manajemen keamanan perdagangan elektronik

Reformasi struktur organisasi manajemen keamanan perdagangan elektronik terutama mencakup diagnosis struktur organisasi, membuat rencana reformasi struktur organisasi, menerapkan reformasi struktur organisasi, menilai struktur organisasi, dan memberikan umpan balik.

Pertama, diagnosis struktur organisasi. Ini termasuk investigasi, analisis, dan penentuan tujuan. Siasati struktur organisasi saat ini dengan melihat bagan struktur organisasi, deskripsi pekerjaan, dan bagan alur bisnis. Setelah itu, analisis struktur organisasi yang ada dilakukan untuk mengidentifikasi perbedaan antara status quo dan harapan status quo. Kemudian, masalah yang perlu diselesaikan diidentifikasi dan dicapai tujuan.

Kedua, menetapkan strategi untuk reformasi organisasi. Mengembangkan dan melaksanakan strategi untuk perubahan struktur organisasi. Dalam rencana reformasi struktur organisasi, harus dijelaskan jenis dan karakteristik masalah, kondisi yang diperlukan untuk menyelesaikan masalah, rute reformasi struktur organisasi dan hasil implementasi, dll. Ada banyak program reformasi struktur organisasi, dan program yang terbaik harus dievaluasi.

Ketiga, lakukan perubahan pada struktur organisasi. Perubahan struktur organisasi adalah sebuah proses, dan untuk melakukannya, ada tiga tahap.

Tahap2; adalah menerapkan perubahan. Pengalaman lanjutan adalah cara yang efektif untuk menerapkan perubahan. Ini memungkinkan karyawan memiliki reaksi mental yang positif terhadap perilaku baru dan secara bertahap menerimanya.Tahap1; adalah menyiapkan perubahan. Setiap pekerja akan mengalami perubahan dalam struktur organisasi. Karena takut bahwa perubahan tersebut akan berdampak pada cara kerja mereka dan pengetahuan dan keterampilan bisnis mereka yang ada, karyawan cenderung menolak. Untuk memastikan transformasi struktur organisasi berjalan lancar, manajer harus memperhatikan strategi transformasi dan metode implementasi; membimbing karyawan untuk menganalisis lingkungan internal dan eksternal, struktur, dan fungsi organisasi; melakukan investigasi yang efektif; dan meningkatkan publisitas untuk memberi tahu karyawan bahwa perubahan diperlukan; dan mendorong semangat karyawan untuk melakukan perubahan struktur.

Tahap2; adalah menerapkan perubahan. Pengalaman lanjutan adalah cara yang efektif untuk menerapkan perubahan. Ini memungkinkan karyawan memiliki reaksi mental yang positif terhadap perilaku baru dan secara bertahap menerimanya.

Tahap 3: Menggabungkan Perubahan Selama reformasi struktur organisasi, tindakan khusus harus diambil untuk meningkatkan sikap dan perilaku baru anggota staf agar mereka dapat berkembang dan berkembang [3]. Misalnya, kami sangat bersemangat untuk menerapkan program pelatihan personel yang disesuaikan dengan perubahan struktur organisasi, sehingga karyawan dapat menguasai pengetahuan dan keterampilan bisnis baru dan siap untuk beradaptasi dengan jabatan baru. Memperbaiki pekerjaan dasar, memperbaiki peraturan, dan mendefinisikan wewenang dan tanggung jawab departemen.

Keempat, penilaian dan komentar tentang struktur organisasi. Analisis struktur organisasi setelah perubahan untuk mengetahui apakah perubahan telah mencapai tujuan, mengevaluasi dampak positif dan negatif dari perubahan, serta masalah yang ada, dan mempersiapkan penyesuaian di masa depan.

BAB 4
Mengendalikan Risiko Informasi dalam E-commerce

Dengan perkembangan pesat teknologi informasi, ada dasar teknis yang kuat untuk pengembangan dan penerapan e-commerce. Namun, keamanan informasi merupakan masalah penting bagi kelangsungan hidup dan perkembangan bisnis e-commerce. Bagian penting dari manajemen keamanan e-commerce adalah mengelola dan mengendalikan ancaman keamanan informasi.

4.1 Proses, Peserta, dan Tanggung Jawab Manajemen Risiko Keamanan Informasi E-commerce

Semakin berkembangnya e-commerce, semakin pentingnya manajemen risiko keamanan data. Proses manajemen yang mengurangi kemungkinan berbagai risiko terjadi atau kerugian yang ditimbulkan ketika risiko tertentu muncul secara tiba-tiba disebut manajemen risiko. Untuk menyediakan program pencegahan kerugian yang efektif, manajemen risiko mencakup kegiatan seperti perencanaan, pengorganisasian, kepemimpinan, koordinasi, dan pengendalian. Ini biasanya menargetkan kejadian yang tidak pasti dengan kemungkinan kecil yang dapat mempengaruhi operasi bisnis. Tujuan manajemen risiko adalah untuk mengurangi dampak potensial ancaman sampai batas yang dapat diterima.

4.1.1 Proses Manajemen Risiko Keamanan Informasi

Manajemen risiko keamanan informasi mengacu pada objek manajemen utama, yaitu "bisnis", seperti data, operator, lingkungan, dan batasnya dari sudut pandang kerahasiaan, integritas, ketersediaan, bukan kredit, atribut keamanan informasi, dan atas dasar koordinasi personel yang komprehensif, teknologi.



Gambar 4.1 Proses spesifik manajemen risiko

manajemen risiko keamanan informasi, komunikasi dan koordinasi, status yang jelas, identifikasi risiko, analisis risiko, penilaian risiko, pembuangan risiko, dan pemantauan dan peninjauan. **Gambar 4.1** menunjukkan prosedur untuk mengelola risiko yang berkaitan dengan keamanan data.

Komunikasi dan konsultasi antara pemangku kepentingan internal dan eksternal diperlukan di setiap mata rantai manajemen risiko keamanan informasi. Oleh karena itu, pada tahap awal penyusunan rencana komunikasi dan konsultasi untuk manajemen risiko keamanan informasi, harus ada rencana yang membahas risiko itu sendiri, penyebabnya, akibatnya, dan langkah-langkah pembuangan risiko. Ini juga harus dikomunikasikan dan dikoordinasikan dengan baik untuk memastikan bahwa dalam proses tanggung jawab manajemen risiko keamanan informasi, para pemangku kepentingan memiliki pemahaman dasar pengambilan keputusan dan bagaimana membuat keputusan.

Status yang jelas mencakup lingkungan yang jelas, seperti penentuan kriteria risiko, kondisi internal dan eksternal yang jelas, dan proses manajemen risiko.

Menemukan, membuat daftar, dan menggambarkan komponen yang berpotensi berbahaya adalah bagian dari proses identifikasi risiko. Tujuannya adalah untuk menemukan peristiwa yang dapat mempengaruhi pencapaian sistem atau tujuan organisasi, serta kerugian apa yang dapat ditimbulkannya. Tujuan lainnya adalah untuk mengetahui tempat, waktu, dan alasan kerugian tersebut dapat terjadi. Tugas identifikasi risiko adalah mengidentifikasi objek entitas, seperti aset informasi, yang harus dilindungi di dalam organisasi, mengidentifikasi ancaman yang mungkin terjadi pada mereka, mengidentifikasi kelemahan dan nilainya, dan mengidentifikasi langkah-langkah keamanan yang telah diambil untuk melindunginya. Metode untuk mengidentifikasi risiko termasuk metode berbasis bukti, seperti daftar periksa dan tinjauan data historis; metode tim sistematis, seperti tim ahli yang menggunakan masalah atau tip terstruktur; dan metode penalaran induktif, seperti analisis risiko dan keefektifan (HAZOP).

Di seluruh siklus manajemen risiko keamanan informasi, pemantauan dan peninjauan dilakukan dengan tujuan menemukan masalah keamanan informasi dengan melacak perubahan pada objek entitas yang dilindungi dan lingkungannya, dan melakukan koreksi yang tepat waktu untuk memastikan proses manajemen risiko keamanan informasi yang berkelanjutan dan berhasil.

4.1.2 Manajemen Risiko Keamanan Informasi dan Tanggung Jawabnya

Orang-orang yang terlibat dalam manajemen risiko keamanan informasi biasanya termasuk otoritas keamanan informasi nasional, departemen yang kompeten dalam bidang

bisnis, pemilik atau operator sistem informasi, kontraktor sistem informasi, layanan keamanan informasi atau lembaga integrasi, dan lembaga yang terkait dengan sistem informasi (misalnya, karena pengadaan sistem, pertukaran dan pembagian data, dll.). Para peserta ini memikul tugas-tugas yang berbeda yang berkaitan dengan manajemen risiko.

Otoritas keamanan informasi negara yang berwenang bertanggung jawab untuk membuat kebijakan, peraturan, dan standar keamanan informasi; mereka juga bertanggung jawab untuk memeriksa dan mengarahkan operasi manajemen risiko keamanan informasi di semua organisasi. Strategi manajemen risiko keamanan informasi departemen harus diusulkan, diorganisasikan, dirumuskan, dan disetujui oleh departemen bisnis yang berwenang. Mereka juga bertanggung jawab untuk memimpin dan mengorganisir penilaian keamanan sistem informasi departemen, menilai apakah risiko dapat diterima berdasarkan hasil departemen, dan memutuskan apakah departemen akan menyetujui sistem informasi untuk beroperasi. Departemen bisnis juga bertanggung jawab untuk memeriksa laporan status keamanan dan melakukan penilaian risiko baru secara teratur atau Pemilik atau operator sistem informasi bertanggung jawab untuk membuat rencana keamanan dan strategi manajemen risiko untuk keamanan informasi dan melaporkannya kepada atasan untuk disetujui. Mereka juga bertanggung jawab untuk mengatur evaluasi mandiri sistem informasi, bekerja sama dengan pekerjaan inspeksi dan evaluasi atau evaluasi yang dipercaya, dan menyediakan dokumen dan sumber daya yang diperlukan. Mereka juga dapat menyarankan penilaian risiko baru kepada otoritas keamanan informasi yang relevan. Kontraktor sistem informasi bertanggung jawab untuk menyerahkan rencana pembangunan sistem informasi kepada pihak-pihak terkait untuk analisis risiko, dan kemudian merevisi rencana sesuai dengan hasil analisis untuk mengendalikan risiko dengan lebih baik dan mengurangi risiko yang ditambahkan pada tahap konstruksi.

4.2 Penilaian dan Pengambilan Keputusan Risiko Keamanan Informasi E-commerce

Penilaian risiko keamanan informasi adalah tahapan penting dalam manajemen risiko keamanan informasi perdagangan elektronik. Ini adalah dasar dan titik awal dari manajemen risiko keamanan informasi perdagangan elektronik. Hasil penilaian risiko keamanan informasi memungkinkan perusahaan perdagangan elektronik untuk menerapkan pengendalian, pemantauan, dan peninjauan risiko selanjutnya. Banyak praktik yang didasarkan pada penilaian risiko telah terbukti efektif dalam manajemen risiko.

4.2.1 Penilaian Risiko Keamanan Informasi

Bisnis utama perusahaan perdagangan elektronik adalah inti dari penilaian risiko keamanan informasi; fokus evaluasi adalah sistem informasi yang terkait dengan bisnis tersebut.

Penilaian Prinsip-prinsip pengendalian, dampak minimum, pemulihan, dan kerahasiaan harus digunakan saat menilai risiko keamanan informasi. Penilaian risiko keamanan informasi adalah proses menilai ancaman keamanan informasi e-commerce dengan menggunakan pendekatan dan teknik ilmiah. Ini secara sistematis menganalisis ancaman dan kerentan sistem komputer, mengevaluasi tingkat bahaya insiden keamanan informasi, dan mengedepankan tindakan penanggulangan dan perbaikan yang ditargetkan untuk melawan ancaman, mencegah dan menyelesaikan risiko keamanan e-commerce, atau mengendalikan risiko dalam kisaran yang dapat diterima. Tujuan dari penilaian risiko keamanan informasi e-commerce adalah untuk mendapatkan pemahaman menyeluruh dan akurat tentang kondisi keamanan informasi perusahaan e-commerce, mengidentifikasi masalah yang timbul, menganalisis kebutuhan keamanan perusahaan e-commerce, dan mengembangkan strategi keamanan informasi yang sesuai dengan kebutuhan saat ini. dan memastikan keamanan informasi perusahaan e-commerce.

Penilaian risiko keamanan informasi terutama untuk mengevaluasi risiko keamanan sistem informasi, dan harus dilakukan sesuai dengan proses penilaian risiko yang diatur dalam Spesifikasi Penilaian Risiko Keamanan Teknologi dan Keamanan Informasi (GB/T 20984-2007). Proses penilaian risiko dapat dibagi menjadi tiga tahap, yaitu identifikasi risiko, analisis risiko, dan penilaian risiko.

1. Identifikasi risiko

Identifikasi risiko terutama melengkapi identifikasi komponen risiko keamanan informasi, seperti aset, ancaman, dan kerentanan, serta identifikasi dan keefektifan langkah-langkah keamanan yang ada. Objektivitas dan keakuratan hasil analisis risiko dipengaruhi oleh kualitas informasi mentah yang diperoleh selama identifikasi risiko. Objektivitas dan keakuratan hasil analisis risiko dipengaruhi oleh kualitas informasi mentah yang diperoleh selama identifikasi risiko.

(1) Persiapan penilaian risiko

Sebelum melakukan identifikasi risiko, diperlukan beberapa persiapan, seperti penetapan lingkungan, investigasi awal, persiapan alat, dan penentuan standar penilaian risiko, ruang lingkup, dan tujuan penilaian. Ini juga mencakup penentuan metode penilaian risiko, pembentukan tim manajemen dan implementasi yang sesuai, dan penyusunan rencana

penilaian risiko. Persiapan alat adalah alat penilaian risiko yang mencakup strategi manajemen keamanan dan sistem manajemen keamanan perusahaan perdagangan elektronik; fungsi dan persyaratan bisnis; struktur dan lingkungan jaringan; batas sistem; data dan informasi; sensitivitas sistem dan data; personel yang mendukung dan menggunakan sistem; dan perangkat keras dan perangkat lunak.

(2) Identifikasi aset

Pertama, aset perusahaan e-commerce diidentifikasi dan disajikan dalam tabel klasifikasi aset. Aset yang diidentifikasi termasuk aset informasi, seperti yang ditunjukkan pada Tabel 4.1, serta aset seperti data, perangkat lunak, perangkat keras, layanan, dan aset personil. Aset-aset ini kemudian diberi nilai dalam penilaian risiko keamanan informasi. Saat menetapkan kerahasiaan, aset dapat dikategorikan ke dalam lima tingkat kerahasiaan, yaitu tinggi, tinggi, sedang, rendah, dan angka 5, 4, 3, 2, 1 menunjukkan tingkat kerahasiaan yang berbeda atau kurangnya kerahasiaan untuk perusahaan e-commerce secara keseluruhan. Saat menetapkan ketersediaan, aset dapat dibagi menjadi tingkat yang sangat tinggi, tinggi, sedang, rendah, dan sangat rendah sesuai dengan persyaratan integritas aset yang berbeda. Nilai integritas dapat diberikan dengan angka 5, 4, 3, 2, 1, sesuai dengan tingkat integritas aset yang berbeda atau dampak kehilangan integritas pada seluruh perusahaan perdagangan elektronik.

Ada kemungkinan bahwa nilai aset dapat diperoleh melalui evaluasi menyeluruh yang didasarkan pada tanggung jawab aset dalam hal kerahasiaan, integritas, dan ketersediaan. Ini dapat dilakukan dengan membandingkan kerahasiaan, integritas, dan ketersediaan aset dan menetapkan salah satu atribut keamanan informasi yang paling penting, atau dengan menimbang penetapan tiga atribut keamanan informasi dan menetapkan hasil perhitungan akhir.

(3) Identifikasi ancaman

Tabel 4. 1 Klasifikasi aset

Jenis Aset	Contoh
Aset Data	Berbagai dokumen digital seperti data dalam media penyimpanan, basis data, dokumentasi sistem, prosedur operasional, panduan pengguna, serta catatan dalam bentuk fisik (kertas).
Aset Perangkat Lunak	- Perangkat lunak sistem: sistem operasi, sistem manajemen basis data, program bahasa pemrograman, serta perangkat lunak layanan lainnya. - Perangkat lunak aplikasi: software pendukung seperti perangkat lunak perkantoran, basis data, dan perangkat lunak lainnya. - Program sumber: kode sumber yang dapat digunakan dan dikembangkan secara individu maupun kolaboratif.

Aset Perangkat Keras	- Peralatan jaringan: router, gateway, switch, dan perangkat jaringan lainnya. - Perangkat komputer: server, komputer desktop, laptop, workstation, serta perangkat portabel lainnya. - Media penyimpanan: hard disk, SSD, tape drive, CD, floppy disk, dan perangkat penyimpanan lainnya. - Jalur transmisi: kabel serat optik, jalur ganda, dan sistem transmisi lainnya. - Peralatan keamanan: firewall, sistem autentikasi identitas, sistem deteksi penyusupan, dan perangkat keamanan lainnya. - Lainnya: printer, mesin fotokopi, pemindai, mesin faks, dll.
Aset Layanan	- Layanan informasi: berbagai layanan eksternal yang memanfaatkan sistem informasi. - Layanan jaringan: koneksi jaringan yang mencakup berbagai infrastruktur dan peralatan jaringan. - Layanan kantor: sistem manajemen informasi yang meningkatkan efisiensi, manajemen konfigurasi, serta pengelolaan aliran file.
Aset Personalia	Sumber daya manusia yang memiliki pengetahuan dan keahlian penting dalam bisnis inti, seperti supervisor pemeliharaan jaringan, manajer proyek aplikasi, dan staf teknis lainnya.
Aset Lainnya	Mencakup reputasi perusahaan, hubungan pelanggan, serta aset tidak berwujud lainnya yang berdampak pada citra organisasi.

Karena ancaman bersifat obyektif, sistem informasi berada dalam bahaya. Wawancara personil dan deteksi alat adalah dua metode utama untuk mengidentifikasi ancaman. Metode pertama memungkinkan bisnis e-dagang untuk dengan cepat memahami semua ancaman terbaru terhadap sistem informasi yang dievaluasi. Namun, pengujian dengan alat khusus diperlukan karena staf mungkin tidak dapat mendeteksi semua ancaman terhadap sistem informasi karena keterbatasan teknis atau kemampuan mereka. Deteksi alat terutama dimulai dari lalu lintas jaringan dan pencatatan dan dilakukan dengan alat analisis tertentu, seperti alat analisis protokol dan alat analisis log. Ancaman terhadap bisnis e-commerce yang sedang dievaluasi oleh sistem diidentifikasi dengan alat analisis yang disebutkan di atas. Risiko fisik, risiko informasi dan jaringan, dan risiko personil adalah tiga sumber utama ancaman. Risiko fisik adalah bahaya yang disebabkan oleh keamanan entitas fisik yang tidak aman, yang lebih sering terjadi dan berpotensi mengancam keamanan sistem informasi. Kesalahan fisik terutama berasal dari kesalahan perangkat keras dan perangkat lunak itu sendiri, kesalahan fasilitas pendukung periferal, serangan fisik, kerusakan lingkungan, dll. Kegagalan perangkat keras dan perangkat lunak mengacu pada kegagalan peralatan dan perangkat keras, masalah jalur komunikasi, kegagalan perangkat lunak, dan masalah lain yang mengganggu operasi bisnis atau sistem. Kegagalan fasilitas pendukung periferal mengacu pada hilangnya fungsi dari fasilitas pendukung periferal. Dampak lingkungan fisik mengacu pada bencana alam dan faktor

lingkungan yang mempengaruhi operasi sistem informasi secara teratur. Selain ancaman fisik, ancaman terbesar bagi keamanan e-commerce adalah ancaman informasi dan jaringan. Kode berbahaya dan virus, jangkauan atau penyalahgunaan yang berlebihan, kebocoran, gangguan, penyangkalan, penyalahgunaan, pencurian, dan serangan jaringan adalah beberapa risiko yang sering terjadi dan membahayakan keamanan sistem informasi.

Serangan jaringan mencakup penggunaan kerentanan jaringan dan masalah keamanan pada perangkat keras sistem jaringan, perangkat lunak, dan data. Seorang penyerang dapat melakukan serangan dari luar perusahaan ke jaringan dan sistem informasi perusahaan, atau mereka dapat melakukan serangan dari dalam perusahaan. Mereka juga dapat melakukan pelanggaran yang melanggar hukum melalui jaringan area lokal atau sistem informasi lainnya milik perusahaan. Selain itu, individu yang bekerja di dalam perusahaan memiliki kemampuan untuk melakukan serangan jarak jauh semu, di mana individu menyembunyikan identitas penyerang dan, setelah memperoleh informasi yang relevan dari target lokal, meluncurkan serangan jarak jauh dari luar, yang menciptakan kesan invasi dari luar. Setiap hubungan dengan aktivitas e-commerce mengandung risiko personel, yang merupakan kategori risiko yang paling luas. Misalnya, orang dapat secara sengaja atau tidak sengaja melakukan ancaman fisik, informasi, dan siber. Risiko yang berkaitan dengan orang dapat berasal dari dalam atau luar perusahaan. Kesalahan pemeliharaan dan kesalahan operasi yang disebabkan oleh kesalahan personel yang relevan atau kesalahan operasi; manajemen personil manajemen yang tidak memadai, termasuk strategi dan sistem manajemen yang tidak sempurna, prosedur yang tidak lengkap, tanggung jawab yang tidak jelas, pengawasan dan tindakan pengendalian yang tidak memadai, dll. Serangan peretasan atau serangan yang disengaja oleh penjahat adalah contoh risiko eksternal.

Nilai ancaman juga akan diberikan setelah identifikasi selesai. Sampai batas tertentu, frekuensi kemunculan ancaman menentukan tingkat keparahan ancaman, sehingga menetapkan frekuensi kemunculan ancaman merupakan langkah penting dalam identifikasi ancaman. Ancaman biasanya dibagi menjadi lima tingkat, masing-masing menunjukkan frekuensi ancaman: lima (sangat tinggi), empat (tinggi), tiga (menengah), dua (rendah), dan satu (sangat rendah). Ancaman lebih sering muncul dengan nilai peringkat yang lebih tinggi. Menghitung frekuensi setiap ancaman dalam proses identifikasi ancaman sangatlah sulit. Ini biasanya terjadi untuk tiga jenis ancaman berikut ini. Pertama, ancaman keamanan informasi yang dilaporkan dalam laporan insiden keamanan informasi; kedua, ancaman yang ditemukan melalui alat deteksi dan berbagai log; dan ketiga, ancaman keamanan informasi yang diumumkan baru-baru ini oleh organisasi yang berwenang di dalam dan luar negeri.

(4) Identifikasi kelemahan

Identifikasi kerentanan adalah bagian penting dari penilaian risiko karena kerentanan yang terancam dapat merusak aset. Dua komponen teknis dan manajemen digunakan terutama untuk menemukan kerentanan. Survei kuesioner, pengujian alat, verifikasi manual, inspeksi dokumen, pengujian permeabilitas, analisis ahli, dan penelitian khusus adalah metode utama yang digunakan. Tingkat kerusakan pada aset, tingkat kesulitan implementasi teknis, dan prevalensi kerentanan dapat digunakan untuk mengatur kerentanan secara hirarkis. Karena banyak kelemahan memiliki hasil atau masalah yang sama, hanya ketika kelemahan ini diberikan bersama-sama yang dapat menentukan seberapa parah kerentanannya. Selain itu, tingkat kerentanan teknis beberapa jenis aset akan dipengaruhi oleh masalah manajemen perusahaan e-commerce. Ada lima tingkat kerentanan, masing-masing menunjukkan tingkat kerentanan yang berbeda: lima (sangat tinggi), empat (tinggi), tiga (menengah), dua (rendah), dan satu (sangat rendah). Tingkat yang lebih tinggi menunjukkan tingkat kerentanan yang lebih tinggi.

(5) Identifikasi dan konfirmasi efektivitas tindakan keselamatan

Langkah-langkah keamanan adalah pendekatan khusus untuk mengelola risiko. Langkah-langkah keamanan terdiri dari berbagai teknik, prosedur, dan mekanisme yang digunakan untuk melindungi aset, melawan ancaman, mengurangi kerentanan, mengurangi dampak dari gangguan keamanan informasi, dan memerangi kejahatan yang berkaitan dengan keamanan informasi. Langkah-langkah pengendalian keamanan secara langsung menentukan potensi insiden keamanan informasi dan cakupan dampak negatifnya. Oleh karena itu, sebelum melakukan analisis risiko, prosedur keamanan yang ada harus diidentifikasi dan keberhasilannya harus dikonfirmasi. Kuesioner atau daftar periksa digunakan untuk mengidentifikasi prosedur keamanan saat ini. Memeriksa apakah tindakan keselamatan yang ada memenuhi harapan yang dinilai berarti mengkonfirmasi keefektifan mereka. Menurut jenisnya, langkah-langkah keamanan dapat dibagi menjadi langkah-langkah teknis dan langkah-langkah normatif. Dalam kebanyakan kasus, langkah-langkah teknis termasuk firewall, deteksi intrusi, audit keamanan, uji keamanan, persetujuan operasi, rencana darurat, dll.

Langkah-langkah teknis biasanya diklasifikasikan menurut tingkat sistem, yaitu jaringan, sistem, aplikasi, dan lapisan data. Analisis prinsip kerja, wawancara dan investigasi, dan uji coba yang tidak berbahaya adalah beberapa cara untuk mengevaluasi efektivitas tindakan teknis. Normatif biasanya mengacu pada pembuatan, pengembangan, operasi, dan pengelolaan sistem informasi sesuai dengan peraturan, standar industri, dan hukum nasional.

Melalui wawancara dan survei, langkah-langkah normatif terutama diidentifikasi. Proses-proses khusus ini meliputi pembuatan formulir evaluasi, pemilihan subjek wawancara, pelaksanaan wawancara dan survei, pengumpulan statistik dan presentasi hasil survei, dan penentuan langkah-langkah normatif berdasarkan hasil statistik.

2. Analisis risiko

Analisis risiko juga diperlukan setelah menyelesaikan identifikasi aset, identifikasi ancaman, identifikasi kerentanan, dan identifikasi tindakan keamanan serta konfirmasi efektivitas.



Gambar 4.2 Isi utama dari analisis risiko

(1) Isi utama dari analisis risiko

Fokus utama analisis risiko adalah untuk mengidentifikasi aset dan menetapkan nilainya; mengidentifikasi ancaman, menjelaskan karakteristiknya, dan menetapkan frekuensinya. Ada kelemahan yang ditemukan dan tingkat kerentanan aset ditentukan. Tentukan kemungkinan insiden keamanan informasi berdasarkan tingkat ancaman dan kerentanan. Hitung dampak peristiwa keamanan informasi pada perusahaan e-commerce, yaitu nilai risiko, berdasarkan tingkat kerentanan dan nilai aset. Hitung kerugian yang disebabkan oleh peristiwa keamanan informasi berdasarkan kemungkinan dan nilai aset.

(2) Metode analisis risiko

Analisis risiko dapat mencakup berbagai metode, seperti analisis kuantitatif dan kualitatif. Ini dapat digunakan untuk menentukan risiko yang dihadapi aset dan dampaknya, serta perbedaan antara tingkat keamanan informasi perusahaan e-commerce saat ini dengan persyaratan keamanannya. Dalam melakukan analisis risiko, tentukan metode analisis apa yang akan digunakan. seperti analisis kuantitatif, kualitatif, atau keduanya. Faktanya, analisis kualitatif dapat digunakan pertama-tama untuk menentukan tingkat risiko umum atau

identifikasi risiko utama, sebelum melanjutkan analisis kuantitatif sesuai kebutuhan karena metode kualitatif biasanya lebih murah dan lebih sederhana.

Metode analisis kualitatif menggunakan tingkat deskriptif untuk menunjukkan kemungkinan insiden keamanan data dan kerugian yang disebabkan oleh insiden keamanan data. Kelebihan metode analisis kualitatif adalah mudah dimengerti, dan kekurangannya adalah penentuan nilai bergantung pada penilaian subjektif. Dengan metode analisis kualitatif, nilai dapat disesuaikan dengan situasi yang sebenarnya dan menggunakan deskripsi risiko yang berbeda. Penyaringan awal mencari risiko yang membutuhkan analisis lebih lanjut biasanya menggunakan analisis kualitatif.

Metode analisis kuantitatif menggunakan berbagai tingkat data untuk menunjukkan kemungkinan insiden keamanan data dan kerugian yang disebabkan oleh insiden tersebut. Kuantifikasi, integritas data, dan efektivitas penggunaan model menentukan kualitas analisis. Banyak kali, metode analisis kuantitatif melihat data historis yang terkait langsung dengan tujuan dan kekhawatiran keamanan informasi; kekurangan metode ini adalah kurangnya data tentang risiko atau kerentanan keamanan informasi yang baru muncul.

(3) Perhitungan nilai risiko

Nilai risiko= R(A, T, V)= R(L(T, V), F(IA, VA)) di mana R adalah fungsi perhitungan risiko, A adalah aset, T adalah frekuensi ancaman, dan V adalah tingkat keparahan kerentanan. Nilai aset yang terkena dampak k Tiga tautan utama ini termasuk dalam perhitungan Var. Pertama, potensi bahaya keamanan data dihitung. Kemungkinan kerentanan untuk memanfaatkan ancaman yang mengakibatkan peristiwa keamanan bergantung pada frekuensi ancaman dan tingkat kelemahan. Kemungkinan peristiwa keamanan informasi = L (frekuensi ancaman, tingkat kerentanan) = L (T, V). Kemudian, untuk menghitung kerugian yang disebabkan oleh peristiwa keamanan informasi, nilai aset ditindaklanjuti oleh peristiwa keamanan informasi dan tingkat kerentanan aset. Nilai risiko dihitung berdasarkan kemungkinan kejadian keamanan informasi dan kerugian yang disebabkan oleh kejadian tersebut. Nilai risiko adalah F (nilai aset yang terkena dampak kejadian keamanan informasi, tingkat kerentanan aset) = F (IA, VA). Untuk menghitung nilai risiko saat melakukan analisis risiko, metode yang paling sesuai dapat dipilih, seperti metode matriks atau metode perkalian.

Untuk memberikan hubungan dua dimensi antara kemungkinan insiden keamanan informasi dan kerugian yang disebabkan oleh insiden tersebut, metode matriks menggunakan matriks dua dimensi. Metode ini sangat fleksibel dan banyak digunakan dalam nilai analisis risiko. Ketika menghitung nilai risiko, biasanya perlu menghitung nilai faktor lain yang ditentukan oleh dua komponen. Faktor-faktor ini, misalnya, menentukan kemungkinan

terjadinya peristiwa keamanan informasi dengan frekuensi ancaman dan tingkat kerentanan, serta tingkat keparahan kerugian dan nilai aset yang diakibatkan oleh peristiwa keamanan informasi. Situasi ini memungkinkan perhitungan nilai risiko dengan perkalian. Kejadian keamanan informasi yang mungkin terjadi dan kerugian yang disebabkannya dapat dihitung dengan membuat fungsi empiris. Metode perkalian sederhana dan mudah dipahami, dan dengan menggunakan perhitungan rumus terpadu, Anda dapat mencapai hasil yang diinginkan. Ketika dua nilai elemen menentukan nilai elemen lain, metode perkalian biasanya digunakan

3. Penilaian risiko

Setelah menganalisis dan mengevaluasi aset, ancaman, kerentanan, dan tindakan keamanan saat ini dalam proses penilaian risiko, penilaian risiko adalah istilah yang mengacu pada analisis risiko yang menyeluruh. Hasil analisis ini dibandingkan dengan kriteria yang diberikan atau dibandingkan dengan hasil analisis berbagai risiko untuk menentukan tingkat risiko. Metode penilaian risiko adalah menghitung dan menganalisis risiko keamanan dari berbagai tingkatan sesuai dengan standar yang berlaku. Tabel 4.2 berisi contoh penilaian risiko. Setelah memilih tindakan pengendalian yang tepat, risiko residu harus dievaluasi untuk risiko yang tidak dapat ditoleransi. Kriteria penilaian risiko menetapkan bahwa ini adalah

Tabel 4. 2 Contoh penilaian

Tingkat risiko	dari keseluruhan risiko	Hasil penilaian risiko secara keseluruhan
Sangat tinggi	≥10%	Tinggi
Tinggi	≥30%	Tinggi
Sedang	≥30%	Sedang
Rendah		Rendah
Sangat rendah		Rendah

Manajemen perusahaan e-commerce untuk membuat keputusan antara meningkatkan langkah-langkah keamanan atau menerima risiko. Laporan penilaian risiko biasanya diberikan setelah hasil risiko keseluruhan ditentukan. Laporan ini menggambarkan seluruh proses dan hasil penilaian risiko. Laporan penilaian risiko mencakup rencana penilaian risiko, prosedur penilaian risiko, analisis identifikasi aset, analisis identifikasi ancaman, daftar kerentanan, identifikasi dan validitas tindakan keamanan yang ada, rencana penanganan risiko, catatan penilaian risiko, dan elemen lainnya. Perusahaan e-commerce juga harus meninjau laporan penilaian risiko secara teratur untuk memastikan bahwa asumsi risiko dan asumsi lingkungan internal dan eksternal masih valid; bahwa hasil penilaian risiko praktis; bahwa teknologi penilaian risiko digunakan dengan benar; bahwa prosedur pengendalian risiko bekerja dengan baik; dan bahwa penilaian risiko mencapai tujuan.

4.2.2 Keputusan Pembuangan Risiko Keamanan Informasi

Setelah penilaian risiko selesai, perusahaan e-commerce harus membuat keputusan tentang bagaimana menangani ancaman keamanan informasi sesuai dengan hasilnya.

1. Proses pembuangan risiko keamanan informasi

Proses pembuangan risiko keamanan informasi adalah kumpulan strategi dan teknik yang digunakan untuk mengendalikan risiko informasi dalam batas biaya yang dapat diterima. Berikut ini adalah prosedur umum untuk menghilangkan ancaman keamanan data.

Pertama, tentukan tujuan pembuangan risiko keamanan informasi. Tujuan pertama harus jelas: mendapatkan paling banyak manfaat dengan biaya paling rendah. Prinsip utama pembuangan risiko keamanan informasi adalah menerima risiko dengan cara yang wajar. Analisis biaya-manfaat dapat digunakan untuk menentukan tujuan pembuangan risiko keamanan informasi.

Kedua, tentukan item mana yang paling penting dalam pembuangan risiko keamanan data. Setiap komponen pembuangan risiko keamanan informasi diberi prioritas berdasarkan tingkat risiko yang ditentukan oleh penilaian risiko. Untuk menghilangkan risiko keamanan informasi dengan prioritas tinggi, item dengan tingkat risiko "5" dan "4" harus ditangani terlebih dahulu. Tindakan yang dilakukan kemudian mulai dari prioritas tinggi hingga rendah.

Ketiga, lakukan analisis biaya-manfaat dari langkah-langkah keamanan. Analisis biaya-manfaat dari langkah-langkah keamanan yang mungkin dilakukan, dan kemudian gunakan analisis tersebut untuk menentukan langkah-langkah keamanan yang memiliki biaya-manfaat terbaik untuk mengurangi risiko bagi bisnis e-commerce.

Keempat, membuat rencana untuk menghilangkan risiko keamanan data. Rencana pembuangan risiko keamanan informasi terutama mencakup hal-hal berikut: item dan materi pembuangan risiko keamanan informasi; tingkat risiko dan tingkat risiko; tindakan keamanan yang direkomendasikan dan prioritas; tindakan keamanan yang diharapkan; sumber daya yang diperlukan untuk melaksanakan tindakan keamanan yang diharapkan; rencana kerja; jadwal kerja; hasil yang diharapkan;

Kelima, menerapkan langkah-langkah keselamatan yang dipilih. Ini berarti mengalokasikan tanggung jawab, memobilisasi sumber daya untuk melaksanakannya, mengevaluasi risiko residual, dan memutuskan apakah akan melakukan pembuangan risiko jika risiko residual masih dalam kisaran toleransi.

Risiko residual adalah bahaya yang mungkin tetap ada pada sistem informasi bahkan setelah tindakan keamanan telah dilakukan. Mengambil langkah-langkah keamanan biasanya hanya mengurangi sebagian dari risiko, dan tujuan untuk mengurangi sebagian dari risiko

biasanya dapat dicapai. Namun, jika risiko ingin dikurangi lebih lanjut, akan ada lebih banyak biaya yang harus dibayarkan. Ini menunjukkan bahwa ada risiko tambahan. Risiko residual harus dipantau secara ketat karena dapat mengakibatkan masalah keamanan data baru di masa depan. Tindakan keamanan tambahan diperlukan jika tingkat risiko residual tidak dapat diterima

2. Metode pembuangan risiko keamanan informasi

Metode yang digunakan untuk mengurangi risiko yang berkaitan dengan keamanan data terutama dibagi menjadi dua kategori: metode kontrol dan metode keuangan. Tujuan utama dari teknik kontrol adalah untuk menghindari dan mengurangi bahaya yang mengancam keamanan informasi dan untuk mengurangi kerugian yang disebabkan oleh bahaya tersebut. Metode yang digunakan untuk melakukan ini termasuk penghindaran risiko, pengalihan risiko, penyebaran risiko, dan pengurangan risiko, serta tindakan pembuangan risiko keamanan informasi lainnya. Metode finansial bertujuan untuk mengurangi biaya yang terkait dengan pemrosesan risiko keamanan informasi melalui pengaturan keuangan. Metode ini mencakup penerimaan risiko dan pengalihan risiko, termasuk pengalihan dari asuransi ke non-asuransi, serta tindakan pembuangan risiko keamanan informasi lainnya.

Pada akhirnya, manajer perusahaan e-commerce harus membuat keputusan tentang pembuangan risiko keamanan informasi ketika mereka membuat keputusan tentang pembuangan risiko keamanan informasi. Selain itu, mereka juga harus mengawasi dan meninjau tujuan pembuangan risiko keamanan data, teknik pembuangan, dan rencana pembuangan. Hal ini dilakukan selama proses pembuangan risiko yang berkaitan dengan keamanan data.

4.3 Implementasi Pengendalian Risiko Keamanan Informasi E-commerce

Pengendalian risiko keamanan informasi sangat penting bagi perusahaan e-commerce untuk mempertahankan standar layanan saat ini dan memperoleh pangsa pasar. Pengendalian risiko keamanan informasi harus diterapkan sesuai dengan strategi pengendalian risiko tertentu dan berdasarkan ukuran biaya-manfaat.

4.3.1 Gambaran Umum Pengendalian Risiko

1. Konsep dan klasifikasi pengendalian risiko keamanan informasi

Pengendalian risiko keamanan informasi mengacu pada manajer yang mengambil tindakan khusus untuk mencegah atau mengurangi kemungkinan terjadinya pelanggaran keamanan informasi atau kerugian yang disebabkan oleh pelanggaran tersebut. Karena kekurangan manajemen dan teknis, sistem e-commerce seringkali memiliki cacat atau celah yang dapat

dieksploitasi oleh manusia atau non-manusia, menciptakan lingkungan yang tidak aman. Perusahaan e-commerce harus menggunakan manajemen risiko keamanan informasi untuk mengurangi risiko keamanan yang berbeda dan mengurangi kehilangan risiko keamanan informasi. Manajemen risiko keamanan informasi adalah komponen penting dari manajemen risiko keamanan informasi.

Ada banyak cara untuk mengkategorikan risiko keamanan data. Ini dapat dibagi menjadi pengendalian risiko tingkat tunggal dan pengendalian risiko multi-level tergantung pada seberapa efektif pengendalian risiko secara teknis. Arsitektur sistem e-commerce mencakup berbagai tingkatan, seperti Internet, Internet luar, Intranet Perusahaan, Jaringan Nilai Tambahan (VAN), perangkat koneksi jaringan (seperti sakelar, router, firewall, dll.), sistem komputer (seperti mainframe, server, dan komputer desktop), aplikasi dan data, dll. Beberapa aplikasi kontrol risiko keamanan informasi digunakan pada satu tingkat, seperti kontrol risiko firewall, antara ekstranet dan intranet perusahaan, sementara yang lain digunakan pada tingkat yang lebih tinggi, antara ekstranet dan aplikasi. Sebagai contoh, setiap kata sandi yang digunakan untuk sistem harus terdiri dari minimal delapan karakter. Kontrol ini dapat dibagi menjadi kontrol pencegahan dan kontrol deteksi berdasarkan tingkat risiko yang terkait dengan keamanan informasi. Pengendalian preventif membantu mencegah kerentanan digunakan dengan membangun fasilitas keamanan atau meningkatkan aturan keamanan. Misalnya, penggunaan berbagai metode sertifikasi daripada metode sertifikasi tunggal memberikan peringatan melalui kontrol risiko deteksi ketika kerentanan sistem digunakan atau aturan keamanan dilanggar. Misalnya, deteksi intrusi, pelacakan audit, pemantauan pemindaian, dan lainnya termasuk dalam kategori teknologi kontrol ini. Kontrol kerahasiaan, integritas, ketersediaan, otentikasi, otorisasi, kepemilikan tanggung jawab, dan kontrol privasi adalah beberapa kategori elemen keamanan berdasarkan kontrol risiko keamanan informasi. Kontrol kerahasiaan berarti pengendalian risiko yang berkaitan dengan penyimpanan, pemrosesan, atau pengiriman data atau informasi. Misalnya, ketika protokol lapisan soket aman (SSL) diterapkan pada server Web, kontrol integritas adalah proses menerima, menyelesaikan, memproses, menyimpan, dan meminta aset informasi dalam kondisi yang konsisten dan tepat melalui prosedur pengendalian risiko. Misalnya, menjaga direktori dan struktur file sistem utama dari perubahan yang tidak sah. Pengendalian Ketersediaan: Prosedur pengendalian risiko yang digunakan untuk memastikan bahwa aset atau sumber daya informasi penting tidak dapat diakses atau diakses. Sebagai contoh, menyebarkan pusat operasi jaringan dan menggunakan alat pemantauan jaringan berkinerja tinggi untuk memastikan ketersediaan jaringan yang optimal. Kontrol otentikasi dimaksudkan untuk memastikan bahwa identitas pengguna sesuai

dengan pengguna aset informasi yang diidentifikasi melalui prosedur pengendalian risiko. Kontrol otorisasi berarti langkah-langkah pengendalian risiko untuk memastikan bahwa pengguna, baik individu maupun komputer, dapat mengakses, mengupdate, atau menghapus sistem atau sumber daya dalam kontrol izin yang wajar. Salah satu contohnya adalah mekanisme otorisasi database yang dapat mengidentifikasi apakah pengguna adalah pengguna aktif. Kontrol atribusi tanggung jawab berarti mengambil tindakan pengendalian risiko untuk memastikan bahwa setiap tindakan dapat dikaitkan dengan proses otomatis atau pengguna tertentu. Log audit, misalnya, dapat melacak data operasi setiap komputer, seperti masuk dan keluar pengguna. Menurut peraturan dan peraturan yang berlaku, mendapatkan, mengakses, mengubah, atau menghapus informasi pribadi dianggap sebagai kontrol privasi.

Menurut cara mereka menangani risiko keamanan data, mereka dapat dibagi menjadi sarana manajemen (normatif) dan sarana teknis. Sarana teknis termasuk teknologi keamanan informasi, keamanan jaringan, keamanan sistem, keamanan aplikasi, keamanan e-commerce, dan teknologi keamanan cloud, antara lain. Sarana manajemen (normatif) terutama didasarkan pada hal-hal berikut: hukum dan peraturan saat ini; standar internasional, nasional, dan industri; persyaratan dan sistem sistem bisnis otoritas industri; tingkat perlindungan keselamatan unit interkoneksi sistem; dan persyaratan kinerja waktu nyata atau langsung sistem.

2. Strategi untuk pengendalian risiko keamanan informasi

Empat kategori strategi pengendalian risiko yang paling umum digunakan dalam industri keamanan informasi: penghindaran risiko, pengalihan risiko, pengurangan risiko, dan penerimaan risiko.

Ketika kerugian akibat risiko tidak dapat diterima dan sulit untuk mengurangi tindakan pengendalian risiko (misalnya, ketika risiko yang teridentifikasi tinggi atau ketika biaya penerapan pembuangan risiko melebihi manfaatnya), strategi penghindaran risiko biasanya digunakan. Strategi ini berusaha untuk menghindari risiko daripada memproses setelah risiko terjadi, dan biasanya digunakan sebagai pilihan terbaik. Secara khusus, strategi ini dapat diterapkan melalui pembuatan sistem manajemen, pengendalian ancaman, penerapan sistem kontrol dan perlindungan teknologi keamanan, dan pelatihan dan pendidikan. Sebagai contoh, manajer risiko harus membuat sistem yang mengontrol penggunaan kata sandi jika mereka harus memastikan bahwa kata sandi diatur dengan ketat. Perusahaan e-commerce harus menghindari ancaman dengan tidak memproses informasi sensitif dalam sistem informasi yang tidak aman. Untuk mencegah kebocoran informasi sensitif, perusahaan harus menghindari menggunakan Internet untuk sistem informasi yang hanya memproses bisnis internal untuk menghindari gangguan berbahaya dari luar dan serangan yang buruk. Perusahaan juga harus

mematuhi peraturan dan hukum untuk memastikan bahwa aktivitas mereka sesuai dengan peraturan dan hukum nasional. Untuk mengurangi risiko sistem, praktik umum adalah menggunakan teknik keselamatan untuk mengontrol dan melindungi sistem. Misalnya, firewall dapat mengurangi ancaman dari luar sistem. Untuk menciptakan lingkungan kerja yang lebih aman dan terkendali, latih dan latih karyawan, dan tingkatkan kesadaran keamanan pelanggan.

Jika risiko tidak dapat dihindari sepenuhnya, metode untuk mengurangi risiko dapat digunakan. Mengurangi risiko berarti mengurangi risiko dengan melakukan tindakan pembuangan risiko tertentu untuk aset informasi yang berisiko. Ketika masukan keamanan lebih kecil daripada kerugian risiko, strategi ini biasanya digunakan. Berbagai hambatan harus dipertimbangkan saat memilih dan menerapkan langkah-langkah pengendalian. Ini termasuk hambatan waktu, hambatan keuangan, hambatan teknis, hambatan operasional, hambatan budaya, hambatan moral, hambatan lingkungan, hambatan hukum, hambatan kemudahan penggunaan, hambatan personel, dll. Mengurangi sumber ancaman, kapasitas ancaman, dan kerentanan adalah metode utama untuk mengurangi risiko. Penggunaan sarana hukum untuk memberikan sanksi terhadap kejahatan komputer, memainkan peran hukum yang membuat jera, dan secara efektif memotivasi sumber ancaman disebut sebagai pengurangan sumber ancaman. Kejahatan komputer termasuk pencurian data rahasia, serangan infrastruktur sistem informasi yang vital, penyebaran virus, konten yang tidak sehat, dan spam. Kemampuan untuk menggunakan teknologi seperti otentikasi identitas untuk mengurangi risiko pemalsuan identitas disebut sebagai mengurangi kemampuan ancaman. Salah satu cara untuk mengurangi kerentanan adalah dengan menambal sistem dengan cepat dan menutup port layanan jaringan yang tidak berguna. Alternatif lainnya adalah dengan meningkatkan kemampuan untuk mendeteksi dan menanggapi risiko dengan membuat rencana tanggap darurat, pemulihan bencana, keberlanjutan bisnis, dll.

Jika risiko tidak dapat dihindari atau dikurangi dan diterima oleh pihak ketiga (pihak yang ditransfer), transfer risiko dilakukan melalui kontrak atau non-kontrak. Strategi ini biasanya digunakan untuk risiko yang memiliki kemungkinan kecil terjadi, tetapi akan berdampak besar pada bisnis e-commerce ketika risiko tersebut terjadi. Transfer risiko terdiri dari kategori asuransi dan non-asuransi. Transfer risiko dapat dicapai melalui penyediaan kembali layanan, outsourcing proyek, pembelian asuransi, atau kontrak layanan dengan pemasok. Menerima risiko adalah istilah yang digunakan untuk menggambarkan ketika perusahaan e-commerce tidak mengambil tindakan lebih lanjut untuk menanggung risiko dan mengalami kerugian. Dalam situasi di mana risiko tersebut jelas memenuhi persyaratan dan strategi e-commerce perusahaan, atau ketika biaya pembuangan risiko jauh lebih besar daripada

manfaatnya, penerimaan risiko biasanya bukan keputusan bisnis yang bijaksana. Secara khusus, risiko penerimaan terbagi menjadi dua kategori: risiko penerimaan pasif dan risiko penerimaan aktif. Perusahaan e-commerce yang menerima risiko pasif biasanya berarti bahwa mereka gagal mengidentifikasi berbagai risiko yang dihadapi atau gagal menerima kerugian risiko secara pasif meskipun mereka gagal mengambil tindakan untuk mengidentifikasi risiko tersebut. Perusahaan e-commerce yang menerima risiko aktif biasanya berarti bahwa mereka mengambil tindakan secara sadar dan tanggap terhadap risiko tersebut. Untuk menentukan apakah perusahaan e-commerce pada akhirnya menerima risiko, mereka harus mempertimbangkan tingkat kerugian risiko dan frekuensi terjadinya risiko.

3. Analisis biaya-manfaat pengendalian risiko keamanan informasi

Menyeimbangkan risiko keamanan informasi dengan keuntungan yang diperoleh harus dilakukan. Perusahaan e-commerce tidak boleh menginvestasikan lebih banyak uang dalam pengendalian dan perlindungan aset daripada nilai aset itu sendiri; proses pengambilan keputusan ini dikenal sebagai biaya-manfaat. Investasi yang dilakukan untuk melindungi aset informasi dikenal sebagai biaya. Menentukan biaya yang diperlukan untuk melindungi dan mengendalikan aset seringkali merupakan tugas yang sulit. Biaya pengembangan dan akuisisi perangkat lunak, perangkat keras, dan layanan; biaya pelatihan, terutama untuk pelatihan staf; biaya implementasi, termasuk instalasi, konfigurasi, pengujian, dan layanan perangkat lunak dan perangkat keras; dan biaya pemeliharaan dan pembaruan. Manfaat ini bermanfaat bagi perusahaan perdagangan elektronik karena mereka membantu mereka menjaga aset mereka. Hasil diwakili oleh nilai ekspektasi kerugian tahunan (ALE). Penilaian aset mencakup evaluasi desain, pengembangan, instalasi, pemeliharaan, pemulihan, dan biaya aktual dan proyeksi untuk mencegah kerugian. Evaluasi aset adalah proses mengalokasikan nilai untuk setiap aset. Ini sangat sulit untuk dilakukan, tetapi beberapa biaya aset dapat dihitung dengan mudah, seperti peralatan yang dibeli, dan beberapa biaya hampir tidak dapat dihitung secara akurat, seperti nilai ekonomi dari informasi utama yang dapat meningkatkan pangsa pasar. Informasi biasanya merupakan objek penilaian aset, yang mencakup biaya untuk membuat, memperoleh, memperbarui, membangun kembali, atau memulihkan informasi, memelihara informasi, nilai untuk pemilik, nilai untuk pesaing, biaya untuk melindungi informasi dan kekayaan intelektual, dan kehilangan produktivitas dan pendapatan perusahaan.

Nilai ekspektasi kerugian tunggal (SLE) = Nilai Aset (AV) × Faktor Eksposur (EF), tetapi metode analisis biaya-manfaat lain menggunakan ekspektasi kerugian tahunan (ALE).

Faktor eksposur termasuk jumlah kerugian yang disebabkan oleh serangan yang diketahui. Nilai ekspektasi kerugian tunggal menghitung nilai kerugian yang disebabkan oleh setiap

serangan, menggunakan nilai aset dan persentase kerugian yang disebabkan oleh serangan yang diketahui. Nilai ini dapat digunakan untuk menentukan nilai ekspektasi kerugian tahunan.

Contoh 1: Nilai aset sebuah situs web e-commerce adalah 100.000 RMB, dan 10% dari kerugian yang diderita situs web akibat serangan peretas (faktor eksposur) adalah dari aset tersebut. Berapa banyak kerugian yang dapat diharapkan dari situs web ini?

Solusi: SLE=AV×EF=100000×10%=10.000

Kedua, nilai kerugian tahunan ekspektasi dihitung. Tingkat kejadian tahunan (ARO) biasanya digunakan untuk menghitung kemungkinan ancaman. Sebagai contoh, kemungkinan serangan terjadi setiap dua tahun sekali adalah 0,5 (50%). Ekspektasi kerugian tahunan (A LE) dapat dihitung dengan rumus berikut: A LE=SLE ARO×

Contoh 2 menunjukkan bahwa sebuah situs web e-commerce memiliki aset senilai 100.000 RMB, dan peretas (faktor eksposur) menyebabkan 10% dari kerugian situs web tersebut. Berapa kemungkinan serangan peretas terjadi setiap tahun?

Solusi: SLE=AV×EF=100000×10%=10000 (yuan), ALE=SLE×ARO=10000×50%=5000 (yuan).

Situs tersebut diperkirakan mengalami kerugian sebesar lima ribu yen setiap tahun. Dengan kata lain, situs e-commerce akan kehilangan 5.000 yuan setiap tahun karena serangan peretas jika tidak meningkatkan keamanannya. Setelah perhitungan biaya tahunan ekspektasi selesai, formula untuk analisis biaya-manfaat adalah sebagai berikut: CBA = ALE (sebelum implementasi tindakan pengendalian) - ALE (setelah implementasi tindakan pengendalian) - ACS. Dimana: ALE (sebelum implementasi tindakan pengendalian) adalah ekspektasi kerugian tahunan sebelum implementasi tindakan pengendalian; ALE (setelah implementasi tindakan pengendalian) adalah ekspektasi kerugian tahunan setelah implementa Analisis biaya-manfaat biasanya dilakukan setelah implementasi prosedur pengendalian risiko keamanan informasi untuk menentukan kapan perlu melakukan perubahan atau optimalisasi.

4.3.2 Tindakan Teknis

Teknik keamanan e-commerce adalah sarana penting untuk menjamin keamanan data e-commerce. Dalam bisnis e-commerce, teknologi keamanan yang tepat harus digunakan untuk melindungi informasi, jaringan, sistem, dan aplikasi, antara lain.

Dalam aktivitas perdagangan berbasis jaringan, berbagai informasi disimpan dan dikirim melalui jaringan dan sistem informasi perdagangan elektronik atau perangkat terkait. Selama proses penyimpanan dan penyebaran, ada risiko yang berbeda terhadap penawaran bisnis, skema bisnis, negosiasi, pembayaran, dan informasi rahasia lainnya. Akan sangat

merugikan aktivitas e-commerce jika informasi ini dicuri. Oleh karena itu, perlu dilakukan tindakan teknis untuk melindungi data pribadi yang dikirim melalui e-commerce.

1. Sistem kata sandi

Plaintext adalah informasi asli yang tidak dienkripsi, dan ciphertext adalah informasi setelah kamuflase diubah. Kriptosistem dan kunci tidak dapat dipisahkan dari proses enkripsi dan dekripsi biasa.

Kriptosistem adalah algoritma yang digunakan untuk enkripsi dan dekripsi, dan kuncinya adalah data kunci yang digunakan untuk melakukan keduanya. Kriptosistem dibagi menjadi kategori simetris dan asimetris tergantung pada apakah algoritma enkripsi dan dekripsi menggunakan kunci yang sama.

(1) Sistem kata sandi simetris

Kriptosistem simetris memiliki kunci enkripsi dan dekripsi yang sama. Selama Anda mengetahui algoritma rahasia plus atau solusi, kriptosistem ini dapat membalikkannya. Pengirim data mendekripsi teks biasa menjadi teks padat, dan penerima mendekripsi teks padat menggunakan kunci yang sama. Kata sandi dapat dibagi menjadi kata sandi aliran dan kelompok tergantung pada mode enkripsi plaintext. Kata sandi kelompok termasuk standar enkripsi data (DES), standar enkripsi data rangkap tiga (3DES), dan standar enkripsi tingkat lanjut (AES). Kata sandi aliran termasuk RC4, RC5, dan SEAL, antara lain.

(2) Sistem kriptografi asimetris

Whitfield Diffie dan Martin Hellman dari Universitas Stanford menyumbangkan gagasan pada tahun 1976. Sistem kriptografi kunci publik dan sistem kriptografi asimetris adalah istilah yang berbeda. Ada dua kunci dalam sistem ini: satu disimpan oleh pemilik kunci, disebut kunci pribadi, dan yang lain dapat dipublikasikan, disebut kunci publik. Kunci publik dan privat sangat terkait. Hanya kunci publik yang sesuai yang dapat mendekripsi data yang dienkripsi dengan kunci publik dan yang dienkripsi dengan kunci privat. Kriptosistem asimetris memiliki algoritma enkripsi dan dekripsi yang dapat diungkapkan. Algoritma pertukaran kunci Diffie Hellman, algoritma ElGamal, dan RSA adalah beberapa algoritma yang banyak digunakan.

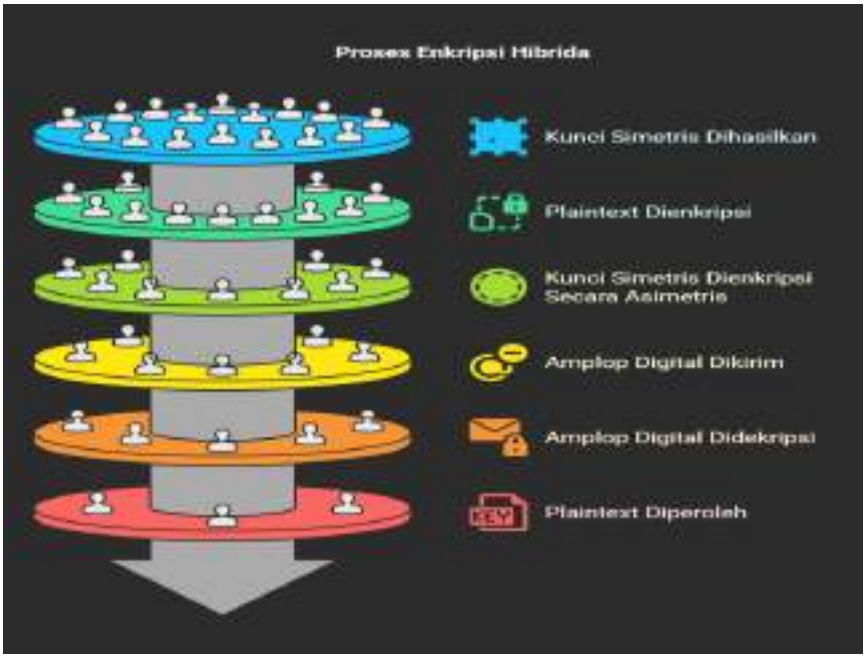
Sistem kriptografi asimetris dapat melakukan dua tugas: enkripsi informasi dan otentikasi identitas, tergantung pada fungsi kunci publiknya. Fungsi enkripsi dan dekripsi data terjadi ketika pengirim mengenkripsi data yang dikirim dengan kunci publik pengirim dan penerima mendekripsi data terenkripsi yang diterima dengan kunci pribadinya sendiri. Dalam proses ini, ketika pihak penerima B menerima informasi yang dienkripsi dengan kunci privat pengirim A, ia dapat mendekripsi informasi tersebut dengan kunci publik A. Jika dekripsi

berhasil, maka B dapat menganggap bahwa pesan itu dikirim oleh A karena informasi yang dienkripsi dengan kunci publik A hanya dapat didekripsi dengan kunci publik A. Jika dekripsi tidak berhasil, maka pesan itu tidak akan dikirim karena kunci privat A tidak dapat didekripsi dengan kunci publik A. Dengan demikian, Ini membentuk dasar teknologi tanda tangan digital. Sistem kriptografi asimetris dapat digunakan untuk banyak hal, seperti tanda tangan digital, otentikasi identitas, berbagi kunci, dan komunikasi rahasia. Sistem kriptografi asimetris dapat membuat tanda tangan digital, yang dapat menggantikan tanda tangan manual tradisional, tetapi algoritma ini tidak cocok untuk mengenkripsi banyak data karena kecepatan yang lambat. Di bidang komersial, seperti penandatanganan menggunakan teknologi tanda tangan digital, ini banyak digunakan. Seseorang dapat mengganggu, memutar ulang, atau memalsukan data sensitif saat mengirimkan surat terbuka. Untuk memastikan keaslian dan integritas informasi, sistem kata sandi asimetris dan sertifikat kunci publik dapat digunakan untuk memverifikasi identitas subjek komunikasi. Informasi rahasia dibagi menjadi n faktor pembagian dan didistribusikan ke n anggota. Hanya faktor pembagian dengan k ($k < n$).

(3) Perbandingan antara sistem kriptografi simetris dan asimetris

Setiap sistem memiliki kelebihan dan kekurangan. Keunggulan komputasi kecil, kecepatan enkripsi yang cepat, dan efisiensi tinggi sistem kata sandi simetris membuatnya populer untuk enkripsi file data. Namun, kelemahan sistem kriptografi simetris adalah sulit untuk menjaga keamanan transmisi, manajemen keamanan, dan tanda tangan digital. Ketika pengirim memberikan informasi terenkripsi kepada penerima, mereka juga harus mengirimkan kunci. Jika kunci diberikan kepada penerima dalam bentuk teks biasa, kunci dapat dicuri. Selain itu, karena kunci selalu harus dikirim dalam bentuk teks biasa, masalah pertukaran kunci atau distribusi menjadi sangat sulit untuk diselesaikan. Dalam kegiatan e-commerce, sulit untuk memastikan transmisi kunci yang aman dalam jaringan komunikasi karena kedua belah pihak tidak bertemu satu sama lain dan mungkin tidak mengenal satu sama lain. Selain itu, item transaksi e-commerce seringkali tidak tetap, yang merupakan salah satu masalah manajemen utama dalam bisnis e-commerce. Untuk menjaga komunikasi yang aman dengan kriptografi simetris, Anda harus membuat sejumlah besar kunci. Sebagai contoh, jika n pengguna dalam jaringan harus berkomunikasi secara rahasia, maka jumlah kunci yang diperlukan adalah $n(n-1)/2$. Selain itu, kunci-kunci tersebut membutuhkan manajemen manusia yang stabil dan dapat diandalkan, sehingga sulit untuk dikelola. Selain itu, sulit untuk menerapkan tanda tangan digital pengguna karena sistem kriptografi simetris digunakan bersama oleh setidaknya dua subjek komunikasi dan tidak memiliki fitur pribadi. Ini karena sulit untuk menentukan sisi mana dari ciphertext yang dibuat oleh entitas komunikasi. Dengan mengubah transfer kunci

menjadi transfer publik, kriptosistem asimetris memecahkan masalah distribusi kunci. Hanya n kata sandi yang diperlukan jika komunikasi rahasia antara n orang diperlukan; ini mengurangi jumlah kunci, memecahkan masalah manajemen kunci, dan menawarkan tanda tangan digital yang efektif. Salah satu kekurangan kriptosistem ini adalah algoritmanya yang cukup kompleks dan kecepatan enkripsi dan dekripsi yang lambat. Oleh karena itu, kriptosistem simetris dan asimetris sering digunakan bersama dalam praktik. Sistem kriptografi hibrida (amplop digital) menggunakan kunci dari kriptosistem simetris untuk mengenkripsi teks plaintext, dan kemudian menggunakan kunci publik dari kriptosistem kunci publik untuk mengenkripsi kunci simetris. Ini memungkinkan enkripsi yang sangat efektif tanpa khawatir tentang pencurian kunci simetris dalam transmisi. Proses khusus dapat dilihat pada **Gambar 4.3**.



Gambar 4. 3 Sistem kata sandi hibrida (amplop digital)

Pengirim A membuat kunci simetris dan menggunakannya untuk mengenkripsi informasi yang akan dikirim. Kemudian, kunci simetris digabungkan dengan kunci publik penerima B dan disebut amplop digital. Setelah dienkripsi oleh kunci publik, pengirim A mengirimkan ciphertext dan amplop digital melalui jaringan ke penerima B. Penerima B kemudian menggunakan kunci privatnya sendiri untuk mendekripsi amplop digital yang dikirimkan oleh pengirim A, sehingga mendapatkan Karena kombinasi sistem kriptografi simetris dan asimetris, amplop digital juga disebut sebagai sistem kriptografi hibrida.

Dalam proses di atas, dua proses enkripsi dan dekripsi sebenarnya dilakukan: enkripsi dan dekripsi informasi itu sendiri dan enkripsi dan dekripsi kunci simetris, yang dilakukan dengan menggunakan kombinasi kriptosistem asimetris dan simetris. Sistem kata sandi asimetris untuk pengelolaan kunci simetris tidak hanya membuat pengelolaan kunci yang

sesuai mudah dan aman, tetapi juga memecahkan masalah otentikasi identitas dan transmisi yang aman. Perlu diingat bahwa kunci simetris biasanya digunakan untuk mengenkripsi informasi plaintext; kunci simetris ini dibuat oleh pengirim informasi, dan mereka juga disebut sebagai kunci sesi. Kunci sesi harus sering diubah untuk mencegah penyerang menggunakan banyak kunci sesi untuk menganalisis ciphertext.

2. Teknologi manajemen kunci

Semua tahap siklus hidup kunci termasuk dalam manajemen kunci, termasuk pembuatan, penyimpanan, pembaruan, pencadangan, distribusi, penghentian, logout, dan lainnya.

Baik klien maupun pusat distribusi kunci (atau otoritas otentikasi) dapat mendistribusikan kunci. Untuk menjaga kunci aman, sebagian besar kunci disimpan di perangkat rahasia, sedangkan bagian lain disimpan di kartu IC atau kartu pintar. Personel khusus menyimpan bagian ini dan memasukkannya ke dalam perangkat saat digunakan. Kunci juga harus diperbarui secara teratur. Pengguna dapat mencadangkan kunci mereka sendiri, kunci oleh pihak ketiga yang dapat dipercaya, atau kunci dalam bentuk komponen atau skema ambang batas. Yang terakhir adalah metode di mana pengguna mencadangkan komponen kunci daripada kunci itu sendiri. Distribusi kunci yang aman ke dua bagian sistem komunikasi disebut distribusi kunci. Sistem kriptografi asimetris dan sistem kata sandi simetris masing-masing menggunakan metode distribusi kunci yang berbeda. Ketika kunci sudah lewat waktu atau dihentikan, kunci harus dihentikan dan diganti dengan kunci baru agar kunci yang dihentikan dihancurkan. Salah satu tujuan pembatalan kunci adalah untuk mengakhiri hubungan hukum antara pemilik kunci dan kunci itu sendiri, serta untuk menghilangkan tanggung jawab entitas atas prosedur penggunaan kunci. Penghancuran kunci berarti menghapus semua kunci dan informasi terkait dari penyimpanan, termasuk kunci dan informasi terkait dalam keadaan cadangan.

3. Teknologi enkripsi jaringan

Sangat penting untuk menjaga keamanan data yang dikirim melalui jaringan komputer, bukan hanya file, kata sandi, informasi kontrol, dan data lain yang disimpan di setiap perangkat yang terhubung ke jaringan. Enkripsi data selama transmisi dan penyimpanan disebut "enkripsi komunikasi". Selanjutnya, enkripsi tautan, enkripsi simpul, dan enkripsi terminal dibagi berdasarkan tingkat komunikasi yang dienkripsi.

Tujuan enkripsi tautan, juga disebut enkripsi online, adalah untuk menjamin transmisi data yang aman melalui tautan antara node jaringan. Ini adalah metode enkripsi yang paling umum dan biasanya digunakan di lapisan fisik dan lapisan tautan model referensi Open Systems Interconnection (OSI), terutama pada perangkat keras. Sebagai jenis enkripsi rantai, jaringan

enkripsi tautan terdiri dari kumpulan simpul koneksi tautan dan semua data dienkripsi sebelum transmisi. Seperti yang ditunjukkan pada **Gambar 4.5**, setiap simpul menerima dekripsi data, menggunakan enkripsi kunci tautan berikutnya, dan kemudian mengirimkannya. Kesalahan pada data yang terhubung ke satu tautan tidak berdampak pada data yang terhubung ke tautan lainnya karena kunci enkripsi yang digunakan oleh tautan berbeda. Node di kedua sisi tautan berbagi satu kunci, dan mode enkripsi manajemen kunci ini agak sederhana. Enkripsi tautan mengenkripsi header dan data yang ada dalam pesan data, sehingga peretas tidak dapat mengakses struktur pesan data, orang yang berbicara, konten, dan waktu.

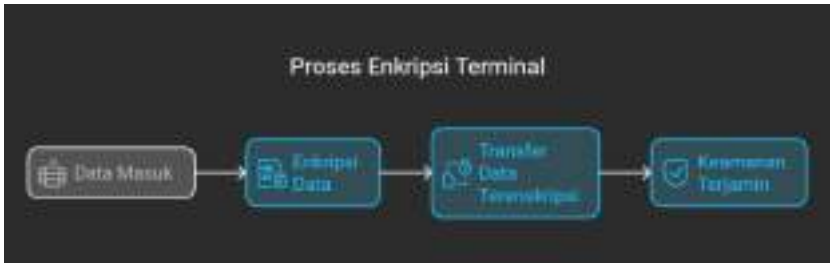
Keuntungan enkripsi tautan adalah sebagai berikut: Pertama, jaringan melakukan enkripsi secara otomatis, sehingga enkripsi tetap transparan bagi pengguna dan data yang dikirim melalui tautan dienkripsi sebelum dikirim. Kedua, node di kedua sisi sambungan berbagi satu kunci, dan ketiga, enkripsi menyediakan mekanisme yang aman untuk aliran sinyal. Kerugian metode enkripsi ini adalah data muncul di node tengah dalam bentuk teks yang jelas, yang membuatnya mudah untuk diakses secara ilegal, dan biaya yang tinggi untuk menjaga keamanan node.

Enkripsi node, yang mirip dengan enkripsi tautan, menggunakan modul keamanan untuk enkripsi dan dekripsi di setiap node perantara, untuk mengatasi kelemahan enkripsi tautan yang menghalangi transmisi teks langsung dari node perantara. Modul keamanan mendekripsi informasi terlebih dahulu dan kemudian mengenkripsinya dengan kunci lain. Ini berarti bahwa data plaintext hanya ada di modul keamanan dan tidak ada lagi yang muncul di node; selain itu, modul keamanan dapat melakukan transfer kunci dari satu kunci ke kunci lain. Namun, setiap node harus menginstal modul keamanan, yang berarti bahwa jaringan publik harus bekerja sama. Selain itu, untuk memudahkan perutean, node hanya mengenkripsi teks pesan data daripada header data. Akibatnya, header dan informasi perutean ditransmisikan dalam teks biasa, yang membuat layanan komunikasi tidak dapat diakses oleh penyerang.

Untuk melindungi data dari sumber ke tujuan, enkripsi ujung-ujung digunakan pada lapisan jaringan dan lapisan transmisi model referensi Open Systems Interconnection (OSI). Metode ini memerlukan bahwa data tetap dalam kondisi ciphertext selama pengiriman dari sumber ke ujung tujuan, sehingga data dienkripsi di sumber dan didekripsi di ujung tujuan. Data pengguna tidak perlu didekripsi di node tengah mana pun.



Gambar 4.4 Enkripsi tautan



Gambar 4. 5 Enkripsi terminal

Seperti yang ditunjukkan pada **Gambar 4.5**, pesan data tidak muncul dalam bentuk teks yang jelas kecuali header di simpul tengah. Kelebihan mode enkripsi terminal adalah sebagai berikut: modul enkripsi terminal hanya digunakan di ujung sumber dan ujung tujuan, dan simpul tengah tidak memerlukan modul enkripsi dan dekripsi, sehingga jumlah modul enkripsi dan dekripsi yang diperlukan lebih sedikit dibandingkan dengan enkripsi tautan. Kedua, pesan data dalam bentuk ciphertext dikirim dari sumber ke tujuan, yang membuatnya lebih aman. Terakhir, metode enkripsi ini dapat diakses oleh pengguna, yang membuatnya lebih fleksibel. Karena metode enkripsi ini hanya mengenkripsi pesan data dan header, mereka tidak dapat melindungi diri dari serangan analisis aliran bisnis. Selain itu, daripada enkripsi tautan, enkripsi terminal membutuhkan lebih banyak kunci.

Teknologi enkripsi jaringan juga tersedia untuk jaringan nirkabel. Dengan transmisi gelombang elektromagnetik, jaringan nirkabel sangat rentan terhadap pencurian data atau situasi serangan perantara. Teknologi enkripsi umum LAN nirkabel termasuk protokol enkripsi nirkabel, protokol akses perlindungan Wi-Fi, dan otentikasi LAN nirkabel dan infrastruktur kerahasiaan. Protokol enkripsi nirkabel kadang-kadang disebut Wired Equivalent Privacy (WEP), yang dirancang untuk membuat jaringan nirkabel dan jaringan berkabel memiliki keamanan yang sama. WEP dapat melindungi keamanan data lapisan sambungan LAN nirkabel, tetapi komunikasi yang aman memiliki banyak cacat keamanan, yang telah digantikan oleh standar keamanan WPA atau WPA2. Protokol akses terproteksi Wi-Fi (WPA) adalah teknologi baru yang mewarisi protokol enkripsi nirkabel dan memperbaiki kekurangannya, termasuk standar WPA dan WPA2. WPA memperkenalkan protokol kontrol akses IEEE802.1×

, protokol otentikasi yang dapat diperluas (EAP), protokol integritas kunci sementara (TKIP), menggunakan vektor inisialisasi yang lebih panjang, meningkatkan mode pencampuran kunci, dan menggunakan kode integritas pesan yang lebih aman (MIC) serta mekanisme keamanan lainnya. Selain itu, WPA menggunakan mekanisme autentikasi pengguna dan algoritme enkripsi baru, memperkuat algoritme pembuatan kunci, dan memecahkan cacat WEP yang mudah dibobol sampai batas tertentu. Selain itu, mode counter-counter cbc-mac (CCMP) yang lebih aman digunakan oleh WPA2, dan algoritme enkripsi RC4 juga digantikan oleh AES yang lebih aman. Infrastruktur autentikasi nirkabel dan privasi (WAPI) adalah solusi keamanan WLAN untuk masalah keamanan WEP. WAPI memanfaatkan teknologi otentikasi dan enkripsi dua arah serta algoritma kriptografi kurva elips dan cipher blok untuk mengidentifikasi identitas peralatan, memverifikasi tautan, mengontrol akses, dan melindungi informasi pengguna dari enkripsi saat transmisi nirkabel. Mode aplikasi satu titik dan terpusat yang dipilih WAPI pada dasarnya menyelesaikan masalah keamanan dan kompatibilitas.

4. Teknologi perlindungan informasi

Teknologi penyembunyian informasi pada dasarnya tidak termasuk dalam kategori kriptografi. Sebaliknya, teknologi enkripsi jaringan mempelajari cara menyandikan informasi rahasia yang ditransmisikan melalui jaringan untuk membentuk teks cipher yang tidak dapat diidentifikasi. Teknologi enkripsi jaringan juga mempelajari cara menyembunyikan informasi rahasia dalam informasi publik dan melalui transmisi informasi publik. Sebenarnya, puisi kepala Tibet Cina kuno adalah implementasi dari gagasan menyembunyikan informasi.

Baik teknologi penyembunyian informasi maupun enkripsi dapat digunakan untuk menyimpan data rahasia; namun, teknologi penyembunyian informasi akan menyembunyikan data dalam data multipembawa sehingga orang lain tidak dapat menemukannya. Salah satu alasan mengapa informasi dapat disembunyikan dalam data multimedia adalah karena redundansi temporal atau spasial, serta pengaruh yang dimiliki sistem pendengaran dan visual manusia terhadap perubahan data. Informasi tersembunyi, yang terdiri dari data yang disematkan; informasi pembawa, yang terdiri dari objek tersembunyi, seperti teks, suara, gambar, dan video, dll; dan pembawa tersembunyi, yang merupakan kombinasi dari informasi tersembunyi dan pembawa. Kunci tersembunyi biasanya digunakan selama proses penyembunyian informasi. Algoritma berbasis domain spasial dan berbasis domain frekuensi adalah beberapa algoritma yang biasa digunakan untuk menyembunyikan informasi.

Berikut ini adalah wilayah utama di mana teknologi penyembunyian informasi digunakan. Pertama, untuk melindungi hak cipta dan mencegah pembajakan karya digital, teknologi penyembunyian informasi sering disebut sebagai "tanda air digital". Penyedia layanan

menyembunyikan informasi identifikasi penyedia layanan dan pengguna dalam bentuk tanda air saat merilis karya kepada pengguna. Jika karya digital disebarkan secara ilegal, penyedia layanan dapat melacak komunikator ilegal dengan mengekstraksi informasi identifikasi mereka. Meskipun jumlah data yang digunakan untuk melindungi hak cipta menggunakan teknologi persembunyian informasi relatif kecil, teknologi persembunyian informasi harus memenuhi persyaratan berikut: kualitas data yang dikirim tidak dapat dideteksi, kekokohan, dan kemampuan untuk dipulihkan setelah gangguan. Selanjutnya, integritas data dan identifikasi keaslian dapat dicapai dengan menggunakan informasi tersembunyi yang tertanam dalam pembawa digital. Ini memungkinkan untuk mengidentifikasi area gangguan dan membedakan keaslian atau integritas karya digital. Anda juga dapat memulihkan zona gangguan jika Anda memasukkan informasi pemulihan. Ketiga, informasi disimpan untuk komunikasi. Teknik penyembunyian informasi mungkin juga rahasia. Teknologi penyembunyian informasi banyak digunakan di bidang militer, bisnis, keuangan, dan lainnya, dan kedua belah pihak dapat mengirimkan informasi sensitif atau rahasia dengan menggunakan surat terbuka. Keempat, validitas yang tidak dapat disangkal Tanda identitas masing-masing pihak dapat disembunyikan dalam data pembawa melalui teknologi penyembunyian informasi, yang memungkinkan validasi identitas. Selain itu, dapat mewujudkan fungsi sehingga kedua belah pihak tidak dapat membantah tindakan mereka. Dengan menggunakan algoritma tertentu, watermark digital dapat dimasukkan ke dalam karya digital multi media, seperti gambar, video, dan audio. Informasi watermark dapat berupa teks, merek dagang, stempel, atau nomor seri, dan sebagainya. Dengan menggunakan informasi watermark ini, orang dapat mengidentifikasi penulis, sumber, versi, pemilik, penerbit, atau pengguna yang sah dari produk digital tersebut. Ada kemungkinan untuk mengekstrak tanda digital dari sinyal host atau untuk mendeteksi keberadaannya. Tanda air digital unik dan dapat diandalkan memberikan bukti kepemilikan yang lengkap untuk produk digital yang memiliki hak cipta. Untuk penyematan tanda air digital, ada algoritme berbasis domain spasial dan berbasis domain frekuensi. Algoritma yang paling sederhana adalah algoritme yang menyematkan tanda air secara langsung ke nilai piksel gambar. Algoritma berbasis domain frekuensi mengubah gambar ke dalam domain frekuensi dengan menggunakan transformasi wavelet atau bentuk trans-kosinus diskrit untuk mengubahnya, dan kemudian menyematkan tanda air digital ke dalam posisi frekuensi tinggi dari konformasi. Kekurangan algoritma ini adalah bahwa ia tidak dapat memproses banyak gambar, seperti blur dan penajaman, sehingga menghancurkan nilai bit efektif terendah (LSB) dalam piksel. Keunggulan algoritma ini adalah ketangguhannya yang tinggi, yang meskipun membutuhkan banyak komputasi, dapat menahan kerusakan yang disebabkan oleh pemrosesan

gambar parsial. Meskipun kedua algoritma ini sederhana, mereka tidak aman, dan tanda air digital dapat dihancurkan dengan mudah. Mengacak posisi watermark digital yang disematkan, seperti LSB atau koefisien frekuensi, adalah solusi. Metode ini memungkinkan tanda air digital yang disematkan untuk tidak mempengaruhi gambar aslinya; mereka tidak dapat diidentifikasi oleh mata manusia, dan tanda air digital tidak dapat dihapus atau dihapus dengan mudah. Tanda air digital biasanya memiliki ciri-ciri berikut: Pertama, tanda air digital dapat dipulihkan tanpa media aslinya. Kedua, menambahkan tanda air digital tidak menurunkan kualitas karya digital secara visual atau pendengaran. Terakhir, tanda air digital tetap lengkap dan tidak berubah setelah perlakuan yang tidak disengaja atau disengaja. Keempat, orang yang tidak diautentikasi tidak dapat mengidentifikasi dan menghancurkan tanda air digital. Kecuali gambar terdistorsi dan kehilangan nilai guna, tanda air digital akan selalu ada. Kelima, meskipun algoritme penyematan tanda air digital dan proses penyematannya, struktur tanda air dan metodenya tetap dirahasiakan.

5. Teknologi enkripsi yang sedang berkembang

Teknologi enkripsi baru seperti enkripsi berbasis identitas, enkripsi berbasis atribut, enkripsi homomorfis, enkripsi anti-kuantum, dan enkripsi ringan muncul sebagai tanggapan atas perubahan dalam kebutuhan enkripsi informasi.

(1) Teknologi enkripsi berbasis identitas

Salah satu penemu RSA, Adi-Shamir, menyarankan teknologi enkripsi berbasis identitas Kriptografi Berbasis Identitas (IBC) pada tahun 1984. Dalam infrastruktur kunci publik (PKI), manajemen sertifikat otoritas (CA) atas sertifikat pengguna menjadi lebih mudah dengan teknologi enkripsi berbasis identitas. Informasi yang dapat mengidentifikasi identitas pengguna, seperti nomor telepon atau email, biasanya digunakan sebagai kunci publik tanpa sertifikat digital yang diberikan oleh agen. Kunci publik pengguna dalam teknologi enkripsi berbasis identitas dapat berupa string apa pun, dan kunci pribadi pengguna dapat dibuat oleh pihak ketiga yang dapat diandalkan, seperti pembuat kunci privat atau PKG. Pengguna A mengirim pesan ke pengguna B dengan kunci publik (alamat email) pengguna B, dan pengguna A mengenkripsi pesan tersebut. Setelah menerima pesan terenkripsi, pengguna B mengautentikasi ke PKG dan meminta kunci privat. Setelah mendapatkan kunci privat, pengguna B mendekripsi pesan dan membaca pesan. Di satu sisi, ia tidak memerlukan sertifikat digital dan menggunakan identitas unik pengguna sebagai kunci publik yang hanya dapat mengidentifikasi mereka. Di sisi lain, ia juga tidak memerlukan agen otentikasi untuk menyediakan generator kunci privat yang dapat diandalkan kepada pengguna. Namun, masalah hosting kunci yang disebabkan oleh enkripsi dapat diselesaikan dengan menggunakan

teknologi pembuatan kunci terdistribusi, teknologi ambang batas, atau teknologi komputasi multi-partai yang aman.

(2) Teknologi enkripsi berbasis atribut

Konsep enkripsi berbasis atribut pertama kali diperkenalkan oleh Sahai dan Waters pada tahun 2005 untuk teknologi enkripsi berdasarkan identitas fuzzy. Enkripsi berbasis identitas adalah lanjutan dari enkripsi berbasis atribut (ABC). Enkripsi ini menggantikan string yang menggambarkan identitas pengguna dengan atribut pengguna yang digambarkan. Karakteristik ini menggantikan string yang menggambarkan identitas pengguna, seperti posisi, unit kerja, dan jenis kelamin. Ada hubungan antara atribut ini dan kunci publik, kunci privat, dan ciphertext pengguna.

Pada enkripsi berbasis atribut, enkriptor membuat kebijakan enkripsi berdasarkan atribut dekriptor dan pesan yang akan dienkripsi. Dekripsi dapat mendekripsi jika fiturnya memenuhi persyaratan enkripsi. Kontrol akses non interaktif dapat diterapkan dengan enkripsi berbasis atribut. Metode enkripsi ini dapat menampilkan setiap izin sistem dengan atribut. Sistem menggunakan otoritas atribut (AA) untuk mengotentikasi atribut setiap pengguna dan memberikan kunci yang sesuai. Server menyimpan semua data sistem dalam bentuk ciphertext. Siapapun dapat mengakses server, tetapi hanya mereka yang memenuhi syarat untuk menggunakan kebijakan akses yang memiliki kemampuan untuk mendekripsi data. Teknologi enkripsi berbasis atribut dibagi menjadi kebijakan kunci berbasis atribut (KP-ABE) dan kebijakan ciphertext berbasis atribut (CP-ABE). Proses pembuatan ciphertext mencakup inisialisasi, pembuatan kunci, enkripsi, dan dekripsi, sedangkan ciphertext berhubungan dengan set atribut. Ciphertext dapat didekripsi dengan sukses hanya jika set atribut yang sesuai dengan ciphertext sesuai dengan struktur akses kunci pengguna. Metode enkripsi berbasis identitas yang disebutkan di atas dapat diklasifikasikan sebagai kp-abe tertentu. Identitas penerima adalah atribut yang tepat untuk ciphertext. Dengan menggunakan strategi asosiasi, dekripsi hanya dapat dilakukan ketika identitas host kunci dan identitas penerima dalam ciphertext konsisten. Ciphertext dalam cp-abe sesuai dengan struktur akses, sedangkan kunci pengguna sesuai dengan set atribut. Pengguna dapat menggunakan kuncinya sendiri untuk mendapatkan kunci dari otoritas otentikasi atribut. Dia hanya dapat menerima izin dekripsi jika set atribut memenuhi struktur akses ciphertext [8].

(3) Teknologi enkripsi homomorfik

Meskipun adopsi dan popularitas komputasi awan dan teknologi enkripsi homomorfik mendorong berbagi data di seluruh dunia, penyimpanan dan alih daya layanan komputasi menimbulkan masalah untuk keamanan dan perlindungan privasi data. Data biasanya disimpan

di cloud dalam bentuk ciphertext untuk mencapai keamanan dan perlindungan data; namun, bagaimana kita dapat menjalankan dan memproses data tanpa mendekripsi teks cipher? Teknologi enkripsi homomorfik dapat menyelesaikan masalah ini. Teori kompleksitas komputasi masalah matematika adalah dasar dari teknologi enkripsi homomorfik. Hasil enkripsi teks biasa setelah operasi sebanding dengan enkripsi teks cipher. Berbeda dengan kebanyakan teknologi enkripsi, enkripsi homomorfis berfokus pada keamanan pemrosesan data. Ini adalah teknologi utama untuk meningkatkan kemampuan pemrosesan ciphertext dan melindungi keamanan data. Ini sangat penting untuk penghitungan dan penyimpanan data ciphertext dalam lingkungan terdistribusi. Misalnya, dalam komputasi awan yang aman dan dipercayakan, daya komputasi server awan pihak ketiga dapat digunakan untuk menghitung data terenkripsi dengan teknologi enkripsi homomorfik. Ini melindungi keamanan dan privasi data serta membuat proses pemrosesan data dan konten data tampak jelas bagi pihak ketiga. Pengguna dapat menyimpan data terenkripsi mereka di server jarak jauh yang tidak dapat diandalkan dan meminta data melalui server jarak jauh jika diperlukan. Setelah kueri dikirim, server jarak jauh mendekripsi hasil kueri dengan kunci publik pengguna, sehingga pengguna dapat mendapatkan data yang diminta sendiri. Selama proses ini, server jarak jauh tidak mengetahui apa pun tentang data yang diminta oleh pengguna. Selain itu, teknologi enkripsi homomorfik dapat digunakan untuk komputasi aman multi-pihak, pemungutan suara anonim, pengambilan ciphertext, akses anonim, perlindungan perangkat lunak, dan banyak lagi.

(4) Teknologi enkripsi anti-kuantum

Teknologi enkripsi anti-kuantum berbasis matematika, teknologi enkripsi DNA berbasis biologi, teknologi enkripsi kuantum berdasarkan fisika kuantum, dan teknologi enkripsi kuantum yang didasarkan pada peralatan fisik kuantum semuanya telah muncul di dunia komputasi kuantum. Secara teoritis, kombinasi distribusi kunci kuantum dan "satu rasionalitas" kuantum mungkin sangat aman. Teori masalah biologis dan kompleksitas komputasi kriptografi menentukan keamanan teknologi enkripsi DNA. Dengan menggunakan DNA sebagai pembawa informasi, kata sandinya memungkinkan enkripsi data, otentikasi identitas, dan tanda tangan digital dengan keunggulan kepadatan penyimpanan yang tinggi dan paralelisme DNA yang tinggi, yang merupakan hasil dari teknologi biologi modern. Namun, kekurangan sistem teoretis membuat teknologi sulit untuk diterapkan dan mahal untuk digunakan. Kriptografi didasarkan pada masalah matematika yang tidak dapat diselesaikan oleh komputer kuantum, yang diciptakan oleh teknologi enkripsi komputasi anti-kuantum. Kriptosistem berbasis kriptografi, tanda tangan digital berdasarkan fungsi hash, kriptosistem

berdasarkan pengkodean koreksi kesalahan, dan kriptosistem multivariat saat ini menjadi fokus penelitian internasional.

(5) Teknologi enkripsi ringan

Teknologi enkripsi yang ringan Dengan pertumbuhan Internet of Things yang pesat, kemampuan pengumpulan data Internet of Things menjadi semakin kuat. Namun, ada banyak masalah yang terkait dengan keamanan. Dalam beberapa tahun terakhir, telah terjadi peningkatan jumlah serangan terhadap Internet of Things, serta peningkatan jumlah insiden kebocoran privasi, penyusupan ilegal, dan kerusakan jaringan lokal. Sangat penting untuk melindungi dan enkripsi perangkat Internet of Things; namun, sebagian besar perangkat memiliki kapasitas komputasi dan penyimpanan yang lemah, dan beberapa membutuhkan kontrol konsumsi energi yang ketat. Akibatnya, teknologi enkripsi konvensional tidak dapat digunakan untuk melindungi perangkat Internet of Things, dan teknologi enkripsi ringan yang cocok untuk digunakan di perangkat Internet of Things diperlukan.

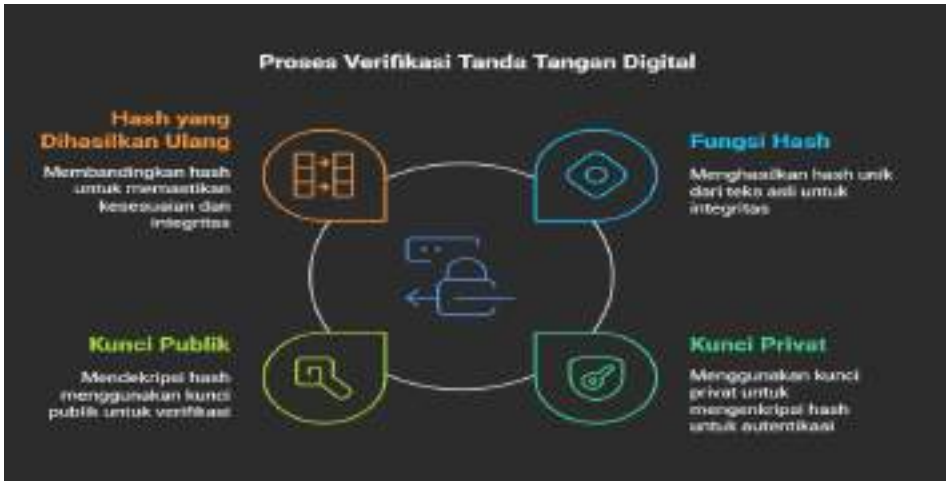
Teknik enkripsi ringan adalah metode enkripsi yang dirancang untuk digunakan pada perangkat yang memiliki sumber daya terbatas. Throughputnya relatif rendah dibandingkan dengan teknologi enkripsi konvensional. Ia mengejar desain algoritme yang tinggi, efisiensi eksekusi, dan penggunaan sumber daya yang lebih sedikit untuk memastikan keamanan yang sesuai. Beberapa teknik enkripsi ringan tidak menyediakan algoritme dekripsi; sebaliknya, beberapa membangun kunci ke dalam perangkat tanpa menggunakan algoritme ekstensi dan distribusi kunci, sehingga meningkatkan efisiensi eksekusi algoritme dalam lingkungan yang terbatas. Dua pendekatan utama saat ini untuk mengembangkan teknologi enkripsi ringan: satu untuk meringankan dan meningkatkan protokol enkripsi yang ada, dan yang lain untuk mengembangkan protokol enkripsi baru. Yang pertama tidak terlalu menantang untuk dirancang, tetapi ada kekurangan, seperti membuatnya ringan atau menimbulkan masalah keamanan baru. Yang terakhir ini sulit untuk didesain dan dianalisis, tetapi sangat fleksibel.

6. Teknologi tanda tangan digital

String yang tidak dapat dipalsukan hanya oleh pengirim informasi, tanda tangan digital adalah digitalisasi tanda tangan tradisional. String ini juga merupakan bukti sah keaslian informasi yang dikirim ke pengirim informasi. Dengan perkembangan jaringan komputer, tanda tangan digital elektronik dapat digunakan oleh banyak bisnis yang sebelumnya menggunakan tanda tangan tulisan tangan. Ini adalah jaminan penting untuk keamanan sistem perdagangan elektronik, cek elektronik, mata uang elektronik, penerbitan elektronik, dan perlindungan kekayaan intelektual.

(1) Prinsip-prinsip dasar tanda tangan digital

Karena kecepatan enkripsi dan dekripsi yang lambat dari kriptosistem asimetris, ringkasan digital dari teks asli (nilai hash) biasanya diperoleh dengan fungsi hash dari teks asli, kemudian dienkripsi dengan kunci pribadi pengirim A, yang kemudian berfungsi sebagai tanda tangan digital pengirim A. Tanda tangan tersebut valid jika keduanya sama, yang berarti file tidak rusak selama transmisi. **Gambar 4.6** menunjukkan prosedur lengkap. Karena nilai hash pesan berbeda, penerima dapat membedakan dengan memverifikasi tanda tangan. Oleh karena itu, bahkan jika penyerang dapat mencegat dan membaca teks asli, dia tidak dapat mengubah konten atau mengganti teks asli dengan informasi lain.



Gambar 4.6 Proses dasar penandatanganan tanda tangan digital

(2) Tanda tangan digital khusus

Dengan berkembangnya jaringan komputer, berbagai metode tanda tangan digital khusus telah muncul, termasuk stempel waktu digital, tanda tangan ambang batas, tanda tangan kelompok buta, dan tanda tangan buta buta.

Jika Anda membutuhkan seseorang atau organisasi untuk menandatangani dokumen, Anda mungkin membutuhkan tanda tangan buta karena mereka tidak tahu apa yang ada di dalamnya. Namun, pada umumnya, saat Anda membuat tanda tangan digital, Anda tahu apa yang ada di dalam dokumen sebelum Anda menandatanganinya. Tanda tangan buta digunakan untuk menjaga anonimitas uang elektronik. Uang elektronik yang dibuat oleh pengguna sendiri hanya dapat digunakan setelah tanda tangan bank; namun, bank tidak dapat melihat konten elektronik yang akan ditandatangani selama proses penandatanganan bank, sehingga tanda tangan buta dapat digunakan. Prinsip dasar penandatanganan buta adalah bahwa hanya jika dua algoritma dapat ditukarkan, tanda tangan buta akan valid. Algoritma enkripsi, yang digunakan untuk menyembunyikan dan mencapai kebutaan, dan algoritma tanda tangan, yang digunakan untuk menandatangani pesan. Konten pesan yang ditandatangani secara buta disembunyikan

dari penandatangan, tidak seperti tanda tangan digital biasa. Selain itu, tanda tangan buta tidak dapat dilacak. Artinya, jika penerima mengungkapkan pesan yang ditandatangani secara buta, penanda tangan tidak dapat mengetahui kapan dia menandatanganinya.

Saat ini, satu bank menerbitkan sebagian besar uang elektronik dalam sistem, dan semua pengguna dan pedagang dalam sistem memiliki rekening di bank yang sama. Namun, pada kenyataannya, beberapa bank dapat menerbitkan uang elektronik di bawah pengawasan bank sentral. J. Camnisch dan M. Stadler membuat program uang elektronik dengan beberapa bank yang berpartisipasi dalam menerbitkan uang elektronik secara anonim melalui internet dengan menggunakan tanda tangan buta kelompok. Menurut rencana tersebut, setiap bank dapat menerbitkan e-cash dengan aman, membentuk sebuah grup dan diawasi oleh bank sentral, yang bertindak sebagai administrator grup.

Tanda tangan gerbang adalah tanda tangan digital yang sah dari file dalam grup yang terdiri dari n anggota, di mana hanya anggota yang lebih besar atau sama dengan t anggota yang digabungkan. Tanda tangan gerbang dapat digunakan dengan menggunakan kunci bersama yang membagi kunci menjadi n bagian, tetapi tanda tangan gerbang hanya dapat direkonstruksi jika lebih dari t bagian digabungkan menjadi satu.

Tanggal dan waktu transaksi adalah data perdagangan yang sangat penting yang secara langsung memengaruhi harga barang yang diperdagangkan. Oleh karena itu, penting untuk melindungi data ini. Stempel waktu digital DTS (Digital timestamp), juga dikenal sebagai stempel waktu keamanan, dibuat oleh agen otentikasi stempel waktu yang dapat diandalkan dengan menggunakan teknologi tanda tangan digital. Teknologi ini dapat digunakan untuk mencegah pengguna melakukan penyangkalan atau penipuan. Stempel waktu digital disediakan oleh otoritas sertifikasi stempel waktu (TSA), sebuah organisasi pihak ketiga yang dapat diandalkan. Proses pembuatan umumnya adalah sebagai berikut: pengguna mendapatkan ringkasan digital dari file stempel waktu dengan menggunakan fungsi hash; TSA memasukkan ringkasan digital ke dalam file, menerima informasi waktu dari file tersebut; kemudian, tanda tangan digital TSA, kunci pribadi, digunakan untuk mengenkripsi file informasi waktu. File voucher digital memiliki stempel waktu digital yang dapat dilihat. Dokumen ini terdiri dari tiga bagian: ringkasan digital dari file yang membutuhkan stempel waktu, waktu ketika otoritas otentikasi stempel waktu menerima ringkasan digital, dan tanda tangan digital dari otoritas otentikasi stempel waktu.

7. Teknologi otentikasi

Autentikasi, juga disebut otentikasi, adalah proses untuk mendapatkan kepercayaan dalam komunikasi jarak jauh yang memastikan identitas asli entitas komunikasi sesuai dengan

identitas yang dinyatakan. Komponen komunikasi dapat berupa individu, perangkat, atau aplikasi sistem komputer yang terhubung ke internet. Tujuan sertifikasi adalah untuk menghentikan individu yang melakukan penipuan, pemalsuan, perusakan, penyangkalan, dan tindakan serupa lainnya.

Autentikasi identitas dan autentikasi pesan adalah dua kategori utama teknologi autentikasi. Autentikasi pesan digunakan untuk memastikan bahwa informasi yang dikirim oleh kedua belah pihak benar dan murni. Tanda tangan digital juga merupakan teknologi autentikasi, yang dapat digunakan untuk memastikan siapa yang mengirimkan pesan. Autentikasi pesan digunakan untuk memastikan bahwa pesan memang berasal dari pengirim yang benar dan tidak diubah, serta memastikan urutan dan ketepatan waktunya. Algoritma enkripsi, fungsi hash, dan kode otentikasi pesan (MAC) adalah beberapa alat yang dapat digunakan untuk menerapkan otentikasi pesan.

Identifikasi identitas mengidentifikasi pengguna atau entitas. Autentikasi identitas berarti memastikan bahwa objek komunikasi tidak menipu atau palsu; dengan kata lain, memastikan bahwa identitas pengguna yang sebenarnya sesuai dengan identitas yang diberikan. Salah satu syarat untuk kontrol akses dan audit adalah autentikasi identitas, yang memungkinkan untuk membedakan pengguna yang sah dari yang ilegal. Keamanan sistem informasi e-commerce dimulai dengan autentikasi identitas. Hanya pengguna yang telah melakukan autentikasi yang dapat menggunakan sistem, sumber daya, dan layanan. Salah satu teknologi yang sangat penting adalah autentikasi identitas, yang membantu mencegah pengguna yang tidak berwenang yang secara aktif menyerang sistem jaringan. Faktor-faktor utama yang dapat digunakan untuk otentikasi identitas adalah sebagai berikut: informasi yang diketahui atau dikuasai, seperti kata sandi; item pengguna tertentu, seperti kartu identitas, kartu pintar, cakram kunci, token, dan alamat IP; dan karakteristik biologis pengguna. seperti suara, sidik jari, dan lain-lain; karena pengguna mengetahuinya, sistem harus membuktikan bahwa pengguna benar-benar memiliki rahasia tersebut; dan karena rahasia yang diketahui kedua belah pihak, kedua belah pihak mengetahui keasliannya. Terkadang beberapa elemen dapat digunakan bersamaan. Misalnya, memiliki kartu bank dan kata sandi untuk menarik uang dari bank adalah salah satu contohnya. Otentikasi dua faktor adalah istilah untuk otentikasi yang menggunakan dua faktor ini. Otentikasi identitas dapat dilakukan dengan berbagai cara. Sebuah otentikasi identitas dapat dibagi menjadi otentikasi identitas satu arah dan dua arah tergantung pada apakah algoritma kriptografi digunakan atau tidak. Selain itu, otentikasi identitas dapat dibagi menjadi otentikasi identitas non-kriptografi dan berdasarkan algoritma kriptografi. Misalnya, otentikasi biometrik, otentikasi pertanyaan-jawaban, dan otentikasi kata sandi memungkinkan autentikasi

identitas yang tidak memerlukan kata sandi. Autentikasi identitas berbasis algoritme kriptografi termasuk jika kedua belah pihak berbagi kunci autentikasi dan melakukan autentikasi yang mirip dengan autentikasi pesan.

8. Sertifikat digital

Karena aktivitas e-commerce semakin berkembang, masalah mengonfirmasi identitas pihak lain dan mencegah penyangkalan setelah identifikasi telah menjadi masalah yang mendesak untuk diselesaikan. Sertifikat digital memungkinkan entitas yang berkomunikasi di Internet untuk mengidentifikasi diri mereka sendiri, seperti sertifikat server yang digunakan untuk mengakses situs keamanan, sertifikat tanda tangan kode otentikasi keamanan perangkat lunak, sertifikat email keamanan yang dikirim, penawaran online, penandatanganan, penandatanganan, toko online, deklarasi bea cukai online, sertifikat identitas pribadi, dan enkripsi, dll.

(1) Pengertian dan kategori sertifikat digital

Identifikasi digital, sertifikat kunci publik, dan sertifikat digital adalah sertifikat digital. Informasi identitas pengguna (seperti pemegang kartu, individu, bisnis, gateway, bank, dll.), kunci publik pengguna, dan file data ditandatangani oleh otoritas otentikasi pihak ketiga yang dapat diandalkan disertakan dalam sertifikat ini. Sertifikasi adalah istilah yang biasa digunakan untuk menggambarkan file data ini di komputer Anda. Seperti kartu identitas, paspor, dan surat izin mengemudi dalam kehidupan nyata, sertifikat digital, yang dikeluarkan oleh lembaga otentikasi, adalah "kartu identitas digital" yang berfungsi untuk membuktikan hubungan antara informasi identitas pemegang kunci publik dan kunci publik. Sertifikat digital memungkinkan identifikasi pertukaran data secara online. Kedua belah pihak yang berdagang secara online dapat menunjukkan sertifikat digital mereka sendiri dan melakukan transaksi berdasarkan sertifikat tersebut. Sertifikat digital dapat dibagi menjadi sertifikat identitas pribadi, sertifikat identitas organisasi atau perusahaan, sertifikat gateway pembayaran, sertifikat server, sertifikat tanda tangan kode, sertifikat email keamanan, dll., tergantung pada apa yang digunakan. Selain itu, tergantung pada cara pasangan kunci dibuat. Kunci privat dan sertifikat yang ditandatangani hanya dapat digunakan dengan tanda tangan digital; mereka tidak dapat dienkripsi atau didekripsi. Modul kata sandi klien harus membuat dan menyimpan pasangan kunci sertifikat, dan kunci publiknya harus digunakan untuk otoritas otentikasi. Kunci privat dan sertifikat enkripsi hanya dapat digunakan untuk enkripsi dan dekripsi; mereka tidak dapat digunakan untuk tanda tangan atau pemeriksaan tanda tangan. Pasangan kunci sertifikat dibuat dan disimpan oleh modul kata sandi klien oleh otoritas otentikasi. Otoritas otentikasi memiliki kemampuan untuk menyimpan salinan pasangan kunci dan memulihkannya jika perlu.

(2) Fungsi sertifikat digital

Enkripsi, tanda tangan, dan identifikasi. Kunci privat dan publik sertifikat digital dapat digunakan untuk tanda tangan dan enkripsi karena sertifikat digital dapat digunakan untuk mengirimkan kunci publik. Sebagai contoh, dengan sertifikat digital, jika Pihak A ingin mengirimkan informasi terenkripsi ke Pihak B dan masing-masing pihak memiliki sertifikat digital mereka sendiri, Pihak A akan mengenkripsi informasi tersebut dengan kunci publik dan mengirimkannya ke Pihak B. Setelah menerima informasi yang dienkripsi, Pihak B akan mendekripsi kunci privat yang sesuai dengan informasi yang dieksplisitkan. Proses otentikasi identitas menggunakan sertifikat digital terdiri dari dua tahap. Pertama, sertifikat digital divalidasi dan benar. Selanjutnya, pemohon adalah pemilik sertifikat digital, yang dapat dilakukan dengan memverifikasi bahwa kunci privat pemohon sesuai dengan sertifikat digital. Untuk autentikasi identitas menggunakan sertifikat digital, ini juga dapat memverifikasi bahwa teks cipher telah dirusak untuk melindungi integritas data. Pertama, A mengenkripsi kunci privat yang sesuai dengan sertifikat digitalnya sendiri untuk mengenkripsi teks asli dan mendapatkan teks rahasia. Selanjutnya, A mengirimkan sertifikat digital dan teks cipher kepada B. Setelah itu, B menerima sertifikat digital dan teks cipher tersebut. Proses khusus terdiri dari memverifikasi tanda tangan sertifikat digital dengan kunci publik oleh lembaga sertifikasi yang mengeluarkannya, serta memverifikasi rantai sertifikat dan masa berlakunya. Keempat, setelah proses verifikasi sertifikat digital selesai, B harus mendekripsi kunci publik sertifikat digital A. Jika dekripsi berhasil, itu menunjukkan bahwa A memiliki kunci privat yang sesuai dengan sertifikat digital dan bahwa A telah melewati proses otentikasi identitas.

(3) Otoritas sertifikat digital

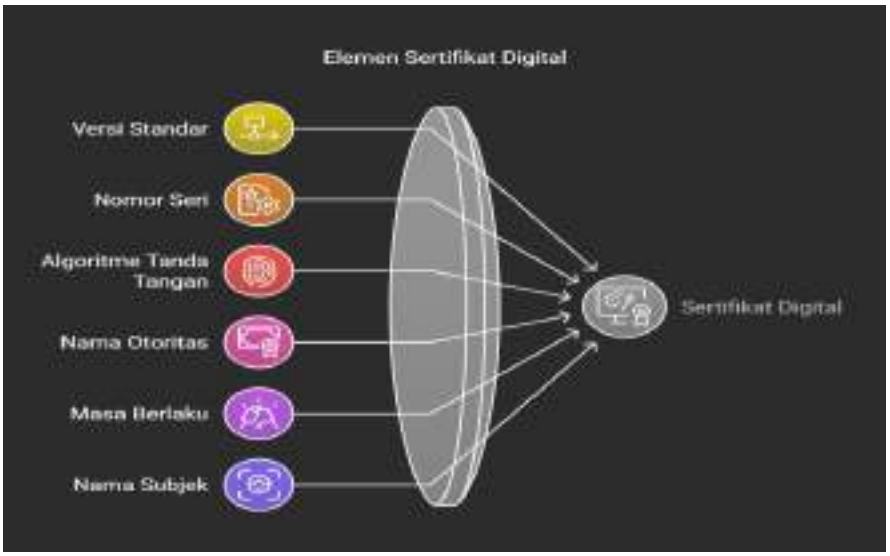
Otoritas sertifikat digital Badan sertifikasi bertanggung jawab untuk mengeluarkan sertifikat digital. Bagian manajemen yang bertanggung jawab untuk menerbitkan sertifikat digital kepada pengguna untuk memastikan bahwa mereka adalah orang yang benar adalah badan sertifikasi. Untuk mencegah pemalsuan sertifikat digital, kunci publik pusat sertifikasi harus dapat diandalkan, dan lembaga sertifikasi harus mempublikasikan kunci publiknya atau memberikan sertifikat elektronik untuk membuktikan bahwa kunci publik tersebut valid. Hal ini menghasilkan munculnya lembaga sertifikasi bertingkat.

(4) Pembuatan sertifikat digital

Otoritas otentikasi menerima informasi identitas dan kunci publik dari calon sertifikat digital dengan aman. Informasi identitas dan kunci publik subjek ditandatangani oleh otoritas otentikasi dengan kunci pribadinya sendiri; selain itu, informasi tanda tangan dilampirkan ke

informasi identitas dan kunci publik subjek. Informasi identitas subjek, kunci publik, dan tanda tangan digital dari badan otentikasi adalah komponen utama dari sertifikat digital ini. Dengan tanggal kedaluwarsa yang ditetapkan, sertifikat digital dibuat dengan tanggal mulai dan waktu penghentian. Pengguna lain akan dapat meminta dan mendapatkan sertifikat digital dari badan sertifikasi.

(5) Isi dan bentuk sertifikat digital



Gambar 4.7 Sertifikat format standar ITU-T X. 509 (versi V1)

Sertifikat digital umumnya menggunakan Standar ITU-T X. 509, dengan format dasar yang ditunjukkan pada **Gambar 4.7**, meliputi hal-hal berikut:

1. Nomor versi: Menunjukkan versi standar ITU-T X.509 yang digunakan untuk sertifikat digital, versi yang umum digunakan saat ini adalah v3, dan nilai defaultnya adalah v1.
2. Nomor seri sertifikat, yang merupakan satu-satunya simbol digital sertifikat, ditetapkan secara seragam oleh otoritas sertifikasi.
3. Pengenal Algoritme Tanda Tangan untuk mengidentifikasi algoritme tanda tangan digital yang digunakan oleh sertifikat digital. Algoritme ini harus sama dengan algoritme tanda tangan di domain sertifikat.
4. Nama X. 500 dari otoritas sertifikasi menunjukkan nama otoritas sertifikasi yang menerbitkan sertifikat digital, yang digunakan untuk membedakan otoritas sertifikasi digital.
5. Masa berlaku menunjukkan masa berlaku sertifikat, termasuk tanggal dan waktu mulai yang valid dari sertifikat digital, serta tanggal dan waktu penghentian.
6. Nama subjek X. 500 menunjukkan nama pemegang sertifikat digital, yang digunakan untuk membedakan pemegang sertifikat digital.

7. Informasi kunci publik subjek mengacu pada informasi kunci publik dari pemegang sertifikat, termasuk nilai kunci publik dari subjek dan pengenal yang mewakili algoritme yang digunakan oleh kunci publik.
8. Nilai tanda tangan digital dari otoritas sertifikasi.

(6) Tampilan sertifikat digital.

Jika sertifikat digital telah diinstal di komputer Anda, Anda dapat melihatnya di browser Internet Explorer dengan mengklik menu Tools dan kemudian perintah Internet Options. Dalam kotak dialog Opsi Internet, klik tombol Sertifikat di tab Konten, seperti yang ditunjukkan pada **Gambar 4.8**. Klik dua kali sertifikat di daftar sertifikat yang sesuai, lalu buka kotak dialog Sertifikat, dan lihat format dan konten sertifikat.



Gambar 4.8 Cara melihat sertifikat digital

9. Infrastruktur kunci publik PKI

Infrastruktur a Infrastruktur kunci publik (PKI), juga disebut sistem kunci publik, adalah infrastruktur keamanan universal yang mengimplementasikan dan menyediakan layanan keamanan yang berbasis teknologi kunci publik. PKI secara teknis memecahkan masalah keamanan seperti non-repudiasi, integritas informasi, dan otentikasi identitas online. Ini adalah infrastruktur yang memberikan layanan keamanan yang dapat diandalkan untuk berbagai aplikasi, seperti e-commerce. PKI didasarkan pada kriptosistem asimetris, menggunakan otoritas sertifikasi sebagai inti, dan menggunakan sertifikat digital sebagai alat untuk menyediakan layanan keamanan dari sudut pandang implementasi [7].

(1) Komposisi infrastruktur kunci public

Struktur infrastruktur kunci publik (PKI) Sistem infrastruktur kunci publik (PKI) biasanya terdiri dari kebijakan PKI, entitas terminal, badan pendaftaran, badan otentikasi, perpustakaan sertifikat/CRL, sistem pencadangan dan pemulihan kunci, dan sistem

pemrosesan sertifikat klien. Strategi Key Cryptography (PKI) adalah dokumentasi rinci dari proses operasional untuk meningkatkan dan mendukung kebijakan keamanan dalam praktiknya. Ini menetapkan pedoman untuk keamanan informasi organisasi dan juga mendefinisikan metode dan prinsip-prinsip penggunaan kriptosistem. Server otentikasi, server direktori, platform PKI, antarmuka aplikasi, basis data, sistem aplikasi keamanan yang dikembangkan sendiri, dan lainnya adalah beberapa contoh sistem perangkat lunak dan perangkat keras. Badan sertifikasi adalah badan eksekutif inti dan entitas konstituen utama PKI, dan bertanggung jawab untuk mengelola dan menerbitkan sertifikat digital. Badan otentikasi berfungsi sebagai dasar kepercayaan dalam transaksi e-commerce. Organisasi menggunakan sistem registrasi dan auditnya sendiri untuk memastikan identitas dan informasi penting lainnya tentang pengguna yang memiliki sertifikat. Ini memastikan bahwa keaslian karakteristik pengguna yang melakukan transaksi melalui internet sebanding dengan keaslian sertifikat. Lembaga sertifikasi melakukan banyak hal, seperti menerbitkan sertifikat, meminta sertifikat, memperbarui sertifikat, mencabut sertifikat, dan mengarsipkan sertifikat. Entitas terminal adalah prinsipal sertifikat atau pihak yang bergantung pada sertifikat, juga dikenal sebagai sertifikat, yang tidak menandatangani sertifikat dengan kunci pribadinya.

Lembaga registrasi adalah anak perusahaan dari lembaga sertifikasi, tetapi dapat diatur dari jarak jauh. Lembaga registrasi menjalankan beberapa fungsi sertifikasi agen, seperti menerima permohonan sertifikat, menyediakan layanan sertifikat tatap muka kepada pengguna, menangani permohonan sertifikat digital dan pembatalan pengguna, meninjau dan mengevaluasi aplikasi sertifikat digital pengguna. Badan pendaftaran berfungsi sebagai perantara antara pengguna dan lembaga sertifikasi, membantu lembaga sertifikasi melakukan tugas sehari-hari. Perlu diingat bahwa kantor pendaftaran adalah pilihan. Perpustakaan sertifikat/CRL adalah basis data informasi publik online yang terutama menyimpan sertifikat dan daftar pencabutan sertifikat (CRL) untuk menerbitkan sertifikat dan CRL ke entitas terminal serta menyediakan layanan kepada publik yang diminta. Perpustakaan sertifikat/CRL memungkinkan penyimpanan, pengelolaan, dan distribusi sertifikat melalui direktori sertifikat; layanan terkait dengan direktori ini dikenal sebagai layanan direktori. Lightweight Directory Access Protocol (LDAP) adalah teknologi direktori yang populer yang memungkinkan banyak pengguna mengakses direktori secara bersamaan. Sistem direktori yang mendukung protokol akses direktori ringan biasanya menggunakan format X.500 Directory Services, yang merupakan metode konvensional untuk membuat direktori internal organisasi atau unit sebagai bagian dari katalog global. Sistem pencadangan dan pemulihan kunci infrastruktur kunci publik perusahaan memungkinkan penyimpanan, pencadangan, dan

pemulihan kunci yang aman, yang merupakan bagian penting dari manajemen kunci. Pemohon sertifikat dapat mengajukan, mengunduh, dan menginstal sertifikat melalui browser melalui sistem pemrosesan sertifikat klien. Anda dapat menggunakan sistem aplikasi yang dikembangkan oleh industri, seperti sistem perbankan atau sekuritas untuk memproses sertifikat klien.

(2) Beberapa infrastruktur kunci publik yang berbeda

Beberapa infrastruktur kunci publik: Infrastruktur kunci publik yang dikelola dan dijalankan oleh satu perusahaan cukup matang dalam praktiknya, tetapi infrastruktur kunci publik yang dijalankan oleh lebih dari satu perusahaan dapat memainkan peran yang lebih besar. Tiga infrastruktur kunci publik multi-perusahaan adalah PKI berbasis PEM, PKI berbasis SET, dan PKI berbasis SSL. PKI berbasis PEM (surat yang ditingkatkan kerahasiaannya, surat yang ditingkatkan kerahasiaannya) dengan struktur pohon adalah standar surat yang ditingkatkan kerahasiaannya yang dibuat oleh Komunitas Internet. Seperti yang ditunjukkan pada **Gambar 4.9**, struktur PKI berbasis PEM memiliki tiga jenis badan sertifikasi.

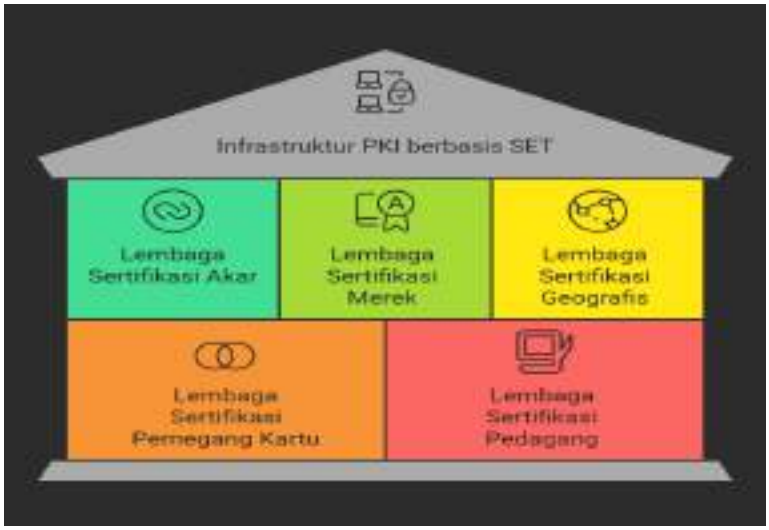


Gambar 4.9 PKI berdasarkan PEM

Di antara mereka, Internet Policy Registration Agency (IPRA) adalah lembaga sertifikasi tingkat tinggi, yang bekerja di bawah naungan International Internet Society. Tingkat kedua adalah Otoritas Sertifikasi Kebijakan (Policy Certification Authority/PCA), yang merupakan satu-satunya lembaga sertifikasi yang disertifikasi oleh Badan Pendaftaran Kebijakan Internet (IPRA). Tingkat ketiga adalah lembaga sertifikasi tingkat rendah (CA).

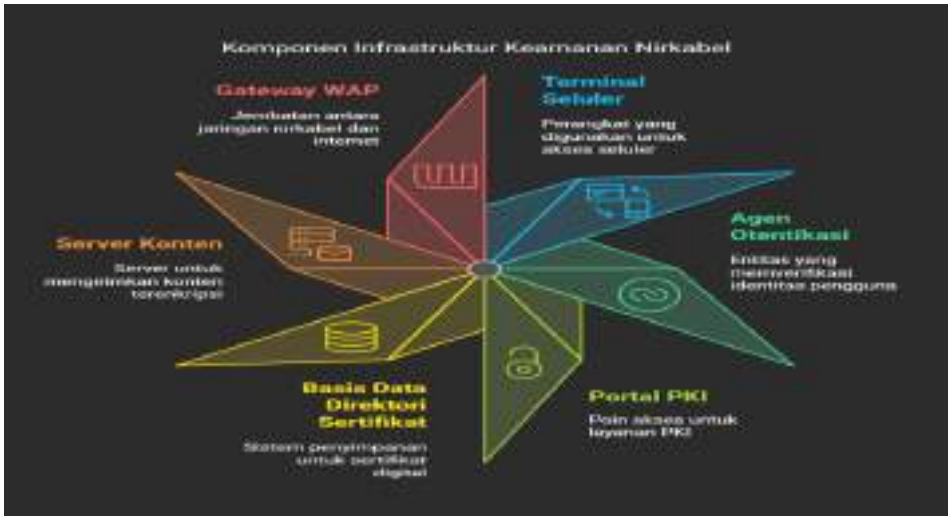
Lembaga sertifikasi ini dapat disertifikasi oleh lebih dari satu kebijakan lembaga sertifikasi (PCA), biasanya sebagai organisasi tertentu atau sebagai area tertentu.

PKI dilakukan berdasarkan SET. Visa dan MasterCard, dua organisasi kartu kredit internasional utama, telah bersama-sama mengembangkan protokol transaksi elektronik yang aman (SET) untuk mengamankan transaksi kartu kredit dalam e-commerce, dan menjadi standar industri yang diikuti ketika sistem pembayaran elektronik melakukan transaksi online. PKI berbasis SET mencakup lembaga sertifikasi akar, lembaga sertifikasi merek, lembaga sertifikasi strategi geografis, lembaga sertifikasi pemegang kartu, lembaga sertifikasi pedagang, dan lain-lain, seperti yang ditunjukkan pada **Gambar 4.10**.



Gambar 4.10 PKI berdasarkan SET

PKI berdasarkan SSL: Protokol Secure Socket Layer (SSL) adalah protokol TCP/IP untuk komunikasi yang aman antara browser dan server. Ini mengadopsi mode "SSL+ form signature", yang memberikan jaminan keamanan yang baik untuk e-commerce.



Gambar 4.11 Diagram struktur infrastruktur kunci publik nirkabel

(3) Radio di Infrastruktur radio dan publik kunci

Infrastruktur publik nirkabel (WPKI) adalah platform keamanan yang didasarkan pada kriptosistem asimetris. Ini memasukkan mekanisme keamanan PKI dalam jaringan kabel ke dalam jaringan nirkabel, dan mencakup berbagai prosedur dan strategi untuk mewujudkan enkripsi dan manajemen kunci dan sertifikat dalam e-commerce seluler. Saat ini, WPKI dapat digunakan untuk perbankan online, keamanan online, dan pengiriman data dan informasi rahasia. Struktur WPKI digambarkan pada **Gambar 4.11**, dan terdiri dari terminal seluler, agen otentikasi, portal PKI, basis data direktori sertifikat, server konten, gateway WAP, dan lainnya.

Perangkat seluler, seperti ponsel pintar atau asisten digital pribadi, yang memiliki kemampuan untuk mengakses jaringan nirkabel dan dilengkapi dengan kartu WIM (Wireless Identify Module). Portal Key Infrastructure (PKI) berjalan pada jaringan kabel seperti gateway WAP dan melakukan tugas yang serupa dengan otoritas registrasi dalam infrastruktur kunci publik; biasanya berfungsi sebagai jembatan yang menghubungkan terminal bergerak dan infrastruktur kunci publik yang sudah ada untuk mengelola informasi registrasi pengguna. Selain itu, portal PKI memungkinkan klien WAP untuk mengirimkan aplikasi sertifikat ke agen otentikasi. Selain itu, portal PKI memberikan akses untuk terminal bergerak dan infrastruktur kunci publik yang sudah ada untuk mengelola informasi.

Seperti lembaga sertifikasi konvensional, lembaga sertifikasi WPKI menyesuaikan format dan permintaan sertifikat untuk memenuhi karakteristik jaringan nirkabel. Basis data direktori sertifikat adalah penerbit sertifikat, seperti server direktori LDAP, yang terutama digunakan untuk mengunduh, sertifikat kueri, menyimpan sertifikat, dan berbagai fungsi lainnya. Selain itu, mereka menawarkan antarmuka eksternal untuk mengunduh sertifikat dan sertifikat kueri. Server konten seperti server situs web badan pengesahan memberikan layanan konten kepada pengguna.

Gateway WAP melakukan dua tugas utama yang berkaitan dengan akses nirkabel. Di satu sisi, itu menangani konversi protokol antara klien dan server sumber, dan berkomunikasi dengan klien melalui protokol WAP dan server sumber melalui protokol Internet standar. Di sisi lain, itu melakukan konversi format data transmisi.

WPKI adalah perluasan dari PKI jaringan kabel, dan keduanya memiliki prinsip dan prosedur bisnis yang sama. Satu-satunya perbedaan utama antara WPKI dan PKI adalah verifikasi sertifikat dan algoritma enkripsi data. WPKI menggunakan X.509 dan dienkripsi dengan algoritma enkripsi kurva elips yang dioptimalkan oleh sertifikat digital untuk beradaptasi dengan lingkungan jaringan nirkabel.

4.3.3 Ukuran Normatif

Dalam pengendalian risiko keamanan informasi e-commerce, terdapat fenomena penekanan pada teknologi dibandingkan manajemen. Para manajer lebih bersedia untuk memperhatikan teknologi keamanan informasi e-commerce, tetapi mengabaikan peran sistem manajemen keamanan informasi e-commerce, peraturan perundang- undangan, standar, dan langkah-langkah normatif lainnya dalam pengendalian risiko. Meskipun langkah-langkah teknis merupakan sarana penting untuk mengendalikan risiko keamanan informasi e-commerce, namun itu bukan satu-satunya cara. Hanya ketika langkah-langkah teknis dikoordinasikan secara efektif dengan langkah-langkah normatif, mereka dapat memainkan peran yang lebih baik.

1. **Langkah-langkah manajemen keamanan informasi**

E-commerce a E-commerce adalah transaksi bisnis yang dilakukan melalui jaringan komputer, dan prosedur manajemen keamanan data terutama mencakup konten berikut.

(1) Sistem pemeliharaan harian sistem informasi e-commerce Sistem pemeliharaan harian sistem informasi e-commerce terutama mencakup sistem manajemen dan pemeliharaan perangkat keras dan perangkat lunak setiap hari, sistem kontrol akses jaringan, sistem pencadangan dan pemulihan, sistem pencegahan virus, kerahasiaan, pelacakan dan audit keamanan, sistem darurat, dll. Perusahaan perdagangan elektronik menggunakan intranet mereka untuk berpartisipasi dalam aktivitas perdagangan elektronik, jadi sangat penting untuk mengelola dan memelihara intranet mereka. Manajemen dan pemeliharaan perangkat keras harian adalah dasar dari manajemen intranet perusahaan. Orang-orang yang bekerja dalam manajemen ruang komputer harus menjaga perangkat keras yang memengaruhi operasi bisnis atau operasi sistem, mencegah kerusakan buatan dan alami, melindungi peralatan periferal sistem, dan memastikan integritas dan ketersediaan perangkat keras.

Selain manajemen dan pemeliharaan perangkat keras, hal-hal berikut juga diperlukan: Perangkat keras, informasi, dan perangkat lunak terkait tidak boleh dibawa keluar dari lokasi perusahaan sebelum diberi wewenang. Perangkat keras yang dipasang di luar tempat kerja harus dilindungi. Sebelum dibuang atau digunakan kembali, perangkat keras yang berisi media penyimpanan diperiksa untuk memastikan bahwa semua data sensitif dan informasi lisensi telah dihapus atau ditulis ulang dengan aman. Perlindungan yang sesuai untuk perangkat keras yang tidak dijaga Simpan media penyimpanan seluler atau kertas dengan benar. Administrator jaringan harus membuat file peralatan perangkat keras, yang mencakup catatan rinci tentang informasi produk perangkat keras, informasi instalasi, dan informasi Internet. Perangkat lunak manajemen jaringan harus diinstal segera untuk memungkinkan pembangunan topologi

jaringan, konfigurasi dan manajemen node sistem jaringan, diagnosis kesalahan sistem, pemantauan dan analisis lalu lintas jaringan, penyesuaian kinerja jaringan, dan tugas lainnya. Jika perangkat keras tidak memiliki perangkat lunak manajemen jaringan, status operasi jaringan harus diperiksa secara manual. Untuk klien dan server, biasanya diperiksa dan dipelihara dengan tangan. Administrator jaringan jalur komunikasi internal harus menyimpan catatan yang akurat tentang kondisi konektivitas jalur komunikasi dan segera menghubungi departemen jalur komunikasi yang disewakan, seperti departemen telekomunikasi, untuk memastikan pemulihan jalur komunikasi dengan cepat.

Kedua, sistem manajemen dan pemeliharaan harian perangkat lunak. Perusahaan perdagangan elektronik harus memiliki sistem manajemen dan pemeliharaan harian perangkat lunak. Manajemen dan pemeliharaan perangkat lunak terutama mencakup perangkat lunak sistem dan aplikasi, seperti sistem operasi dan sistem manajemen basis data. Sistem operasi harus mematuhi prinsip izin minimum dan berbagi maksimum, serta mengambil tiga langkah manajemen keamanan, termasuk kontrol isolasi, kontrol akses, kontrol aliran informasi, dan audit. Selama pemeliharaan sistem operasi, bersihkan file log dan file sementara secara berkala, atur sistem file secara berkala, mendeteksi status aktivitas dan registrasi pengguna di server, menangani kesalahan operasional, dll. Lapisan inti basis data termasuk basis data jaringan dan non-jaringan, yang memiliki fungsi seperti enkripsi, kontrol klasifikasi, dan desain pemulihan bencana.

Ketiga, pengelolaan akses ke jaringan. Perusahaan e-commerce harus membuat sistem kontrol akses jaringan. Kontrol Akses Jaringan adalah lapisan pertama kontrol akses jaringan, yang mencakup identifikasi dan verifikasi nama pengguna, identifikasi dan verifikasi kata sandi pengguna, dan memeriksa batasan akun default pengguna. Validasi nama pengguna dan kata sandi merupakan garis pertahanan pertama kontrol akses. Administrator jaringan harus memiliki kemampuan untuk mengatur waktu dan akses jaringan, membuat, memelihara, dan menutup akun pengguna, mengaudit, melacak, dan memantau akses pengguna, dan membatasi jumlah workstation yang dapat digunakan.

Keempat, sistem pemulihan dan pencadangan. Perusahaan e-commerce harus memiliki sistem pencadangan dan pemulihan untuk memastikan ketersediaan sistem bisnis yang tinggi. Pencadangan mencakup pencadangan sistem, pencadangan data, dan pencadangan jaringan. Pencadangan sistem terutama digunakan untuk menyimpan informasi, perangkat lunak, dll. Pencadangan data terutama menggunakan berbagai media penyimpanan. Tujuan pencadangan adalah untuk meminimalkan kerugian data jika terjadi kegagalan atau ancaman. Pencadangan data dapat dilakukan secara otomatis oleh sistem atau secara manual oleh pengguna.

Pencadangan jaringan berarti menggunakan server tertentu di jaringan sebagai server cadangan, menghubungkannya ke perangkat penyimpanan berkapasitas besar, dan menginstal perangkat lunak server yang mengatur penyimpanan data jaringan. Pemulihan berarti bahwa data cadangan atau sistem cadangan dapat digunakan untuk memperbaiki sistem informasi e-commerce yang rusak karena kecelakaan atau kesalahan operasional.

Kelima, sistem pencegahan virus. Perusahaan e-commerce harus membangun sistem pencegahan virus dan mengambil dua langkah: langkah-langkah teknis untuk mencegah virus dan langkah-langkah normatif untuk membangun sistem yang secara teratur mendeteksi dan membersihkan virus. Saat mengunduh perangkat lunak, gunakan situs web yang sah dan jangan kunjungi situs web ilegal; hati-hati saat mengunduh lampiran email; gunakan antivirus setelah terdeteksi jika ada file yang dapat dieksekusi dalam lampiran email; dan gunakan perangkat lunak jaringan asli.

Keenam, sistem kerahasiaan: perusahaan e-commerce harus membuat sistem yang melindungi data mereka. Pasar, produksi, keuangan, pasokan, dan rahasia bisnis lainnya terlibat dalam transaksi online, jadi perlu membagi tingkat keamanan informasi, menentukan fokus keamanan, dan membuat langkah-langkah kerahasiaan yang tepat. Mereka biasanya membagi keamanan data menjadi tingkat sangat rahasia, tingkat menengah, dan tingkat rahasia. Misalnya, situs web dan kata sandi rahasia hanya dapat diakses oleh staf manajemen senior; situs web dan kata sandi rahasia hanya dapat diakses oleh staf tingkat menengah ke atas; dan konsumen dapat melihat situs web dan kata sandi rahasia. Namun, perlu ada prosedur perlindungan untuk mencegah penyusupan "peretas". Pembuatan, pengiriman, dan penghancuran kunci juga harus diawasi selain keamanan dan manajemen hirarki informasi; kunci juga harus diganti secara teratur.

Ketujuh, sistem pelacakan dan audit keamanan. Perusahaan e-commerce harus membuat sistem audit keamanan untuk mengawasi semua peristiwa dan perilaku. Mereka juga harus membuat sistem pelacakan untuk mencatat seluruh proses operasi sistem melalui log sistem perdagangan jaringan untuk mengawasi dan memelihara operasi sistem. Selain itu, sistem informasi e-commerce akan secara otomatis menghasilkan file log yang mencakup informasi seperti tanggal operasi, mode operasi, waktu login, waktu berjalan, dan konten transaksi.

Kedelapan, sistem tanggap darurat. Perusahaan e-commerce harus membuat sistem darurat dan mengembangkan rencana manajemen keselamatan dan darurat untuk segera menerapkan rencana yang sesuai jika terjadi kecelakaan atau peristiwa bencana,

menghilangkan kesalahan, mengembalikan sistem ke kondisi normal sesegera mungkin, dan meminimalkan kerugian.

(2) Memeriksa keadaan saat ini sistem informasi e-commerce. Analisis kesehatan sistem informasi e-commerce mengacu pada pengecekan apakah penggunaan berbagai sumber daya dalam sistem memenuhi tujuan yang diharapkan dan menentukan arah perbaikan dan perluasan sistem. Kinerja sistem menentukan keputusan mana yang harus dibuat oleh manajer: mengembangkan sistem baru atau memperbaikinya.

2. **Organisasi standardisasi keamanan informasi**

Saat ini,a Sekitar ratusan organisasi internasional dan regional saat ini terlibat dalam pembuatan standar teknis. Berikut ini adalah beberapa organisasi utama yang bertanggung jawab atas standarisasi keamanan data.

(1) Organisasi Internasional untuk Standardisasi Keamanan Informasi Satuan Tugas Rekayasa Internet (IETF) adalah organisasi yang paling terkenal di dunia untuk standardisasi teknologi Internet. Tugas utama IETF adalah mengatur pengembangan dan perumusan standar teknis yang berkaitan dengan Internet. Saat ini, IETF adalah sumber sebagian besar standar teknis Internet internasional. ECMA International adalah lembaga yang didirikan untuk menetapkan standar untuk informasi dan komunikasi yang berbasis anggota. Sampai tahun 1994, European Computer Manufacturers Association (ECMA), yang berbasis di Jenewa, Swiss, diminta untuk menyelidiki standar ICT dan menerbitkan laporan teknologi.

(2) Lembaga Standar Nasional Amerika (ANSI) adalah kelompok standar sipil nirlaba yang didirikan oleh perusahaan, pemerintah, dan kelompok lain. Ini adalah organisasi sukarela yang bertanggung jawab atas standarisasi keamanan informasi negara yang relevan. Institut Standar dan Teknologi Nasional AS (NIST) dimiliki oleh Departemen Perdagangan AS dan bertanggung jawab atas pemrosesan data non-rahasia dan sensitif yang dimiliki oleh pemerintah federal AS. Britain Standard Institute (BSI) adalah organisasi nirlaba yang menyediakan layanan standar internasional dan terdiri dari lima bisnis yang saling melengkapi: penelitian dan pengembangan standar, penyediaan informasi teknis standar, pengujian produk, sertifikasi sistem, dan layanan pendidikan dan pengembangan standar. Selain itu, negara-negara maju seperti Kanada, Jepang, Korea Selatan, dan lainnya telah membentuk kelompok yang bertanggung jawab untuk menetapkan standar keamanan informasi.

(3) Organisasi Standardisasi Keamanan Informasi China: Organisasi Standardisasi Keamanan Informasi Tiongkok secara independen membuat standar keamanan informasi yang sangat penting untuk menjaga keamanan informasi di Tiongkok. Pekerjaan standarisasi China menerapkan sistem manajemen yang menggabungkan manajemen terpadu dengan pembagian

tugas dan tanggung jawab. Administrasi Standardisasi akan berada di bawah otorisasi Dewan Negara dan di bawah pengawasan Negara untuk Regulasi Pasar. Komite Teknis Standardisasi Keamanan Informasi Nasional didirikan pada tahun 2002 oleh Administrasi Standardisasi. Ini adalah organisasi tingkat atas untuk pekerjaan standardisasi keamanan informasi di China. Tugasnya adalah memberikan pedoman untuk standardisasi keamanan informasi kepada administrasi standardisasi nasional, memberikan saran kebijakan dan teknis, dan mengatur teknologi standardisasi yang terkait dengan keamanan informasi, serta ruang lingkup pekerjaan dan sumber daya manusia. WG1, WG3, WG4, WG5, WG6, WG7, dan Satgas Keamanan Big Data WG-BDS adalah tujuh kelompok kerja yang tergabung dalam Komite Teknis Nasional Standarisasi Keamanan Informasi. WG1 bertanggung jawab untuk koordinasi dan standarisasi sistem keamanan informasi. Tugasnya adalah mempelajari sistem standar keamanan informasi, mengikuti tren perkembangan standar keamanan informasi di tingkat internasional, mempelajari dan menganalisis kebutuhan penerapan standar keamanan informasi di tingkat domestik, dan mempelajari dan mengajukan ide untuk proyek baru. WG3 adalah kelompok kerja teknologi kriptografi, yang bertanggung jawab atas penelitian dan pengembangan algoritma kriptografi, modul kriptografi, dan standar manajemen kunci. WG4 adalah kelompok kerja identifikasi dan otorisasi, yang bertanggung jawab atas analisis, penelitian, dan pengembangan infrastruktur kunci publik (PKI) / Infrastruktur Manajemen Otorisasi dan Infrastruktur Manajemen Otorisasi luar negeri (PMI). WG5 adalah kelompok kerja evaluasi keamanan informasi. Tugas mereka adalah untuk memeriksa kondisi saat ini dan tren dalam dan luar negeri dalam pengembangan standar evaluasi, mengawasi proyek standar evaluasi, dan membuat rencana yang sesuai. WG6 adalah kelompok kerja standar keamanan komunikasi yang bertanggung jawab untuk memeriksa kondisi dan tren saat ini dalam standar keamanan komunikasi, meneliti dan mengusulkan sistem untuk standar tersebut, dan merumuskan dan merevisi standar tersebut. WG7 adalah kelompok kerja manajemen keamanan informasi yang bertanggung jawab untuk mempelajari sistem standar manajemen keamanan informasi dan merumuskan standar manajemen keamanan informasi. SWG-BDS adalah gugus tugas standar keamanan data besar yang bertanggung jawab atas pengembangan standardisasi keamanan terkait data besar dan komputasi awan, termasuk penelitian tentang persyaratan standardisasi, penelitian, dan mengedepankan peta jalan pengembangan standar.

Biro Keamanan Negara, Komite Teknis Standardisasi Keamanan Sistem Informasi dari Kementerian Keamanan Publik, dan Komite Kerja Teknis Jaringan dan Keamanan Informasi dari Asosiasi Standardisasi Komunikasi Tiongkok adalah beberapa organisasi manajemen standar keamanan informasi di Tiongkok. Salah satunya adalah Biro Keamanan Negara, yang

bertanggung jawab untuk mengawasi, mengeluarkan, dan memastikan standar keamanan negara. Manajemen kerahasiaan China bergantung pada undang-undang dan peraturan kerahasiaan nasional. Dalam standar industri keamanan publik Tiongkok, komite teknis Standardisasi Pemrosesan.

Komputer dan Informasi dari Kementerian Keamanan Publik bertanggung jawab atas pengelolaan teknis terpusat standar informatisasi keamanan publik. Komite Kerja Teknologi Keamanan Jaringan dan Informasi dari Asosiasi Standardisasi Komunikasi China bertanggung jawab atas pengaturan, penelitian, dan pembuatan standar dan spesifikasi teknis untuk industri komunikasi terkait keamanan jaringan dan informasi.

3. **Standar keamanan informasi**

Panduan ISO No. 2 (versi 4), yang dikeluarkan oleh Organisasi Internasional untuk Standardisasi pada bulan Juli 1983, mendefinisikan standar sebagai spesifikasi teknis yang dibuat bersama oleh pihak-pihak yang terkait berdasarkan pencapaian ilmiah dan teknologi serta pengalaman yang telah maju atau yang pada dasarnya disetujui oleh pihak-pihak yang terkait atau dokumen publik lainnya, yang dimaksudkan untuk mempromosikan kepentingan publik yang terbaik. Standar di China didefinisikan sebagai ketentuan terpadu tentang hal-hal dan konsep yang berulang yang didasarkan pada temuan ilmiah, teknis, dan praktis; ini disusun oleh pihak-pihak terkait, disetujui oleh pihak yang berwenang, dan diterbitkan dalam bentuk tertentu untuk berfungsi sebagai pedoman dan dasar untuk kepatuhan bersama.

(1) Pengkategorian dan penggolongan standar Penilaian standar: Standar Tiongkok dibagi menjadi empat tingkat, menurut Undang-Undang Standarisasi Republik Rakyat Tiongkok: Standar Nasional, Standar Industri, Standar Lokal, Standar Kelompok, dan Standar Harga. Perumusan, pengujian, dan persetujuan standar nasional diawasi oleh Departemen Administrasi Standardisasi Dewan Negara. Departemen administrasi Dewan Negara yang relevan harus menetapkan standar perdagangan dan melaporkannya ke Departemen Administrasi Standardisasi Dewan Negara untuk dicatat. Departemen administrasi standardisasi pemerintah provinsi harus membuat standar lokal, lalu diserahkan kepada departemen administrasi standardisasi Dewan Negara dan departemen administrasi terkait Dewan Negara untuk dicatat. Standar perusahaan harus dibuat, diperiksa, disetujui, dan dikeluarkan oleh pemimpin yang kompeten yang disahkan oleh perwakilan hukum atau perwakilan hukum, dan dikelola secara seragam oleh departemen yang disahkan oleh perwakilan hukum perusahaan. Departemen administrasi standarisasi lokal dan departemen administrasi terkait harus diberitahu tentang standar produk perusahaan. Standar dapat dikategorikan menurut berbagai kategori. Pertama, standar dapat dibagi menjadi standar

internasional, standar regional, standar nasional, standar industri, dan standar perusahaan berdasarkan seberapa luas dan luasnya standar tersebut. Kedua, batasan standar dapat membagi standar menjadi yang disarankan dan yang wajib. Standar yang harus diikuti adalah standar yang ditetapkan oleh standar nasional, standar industri, undang-undang, dan peraturan administratif lainnya. Ketiga, standar dapat dibagi menjadi standar dasar dan standar umum berdasarkan posisinya dalam sistem standar. Keempat, standar dapat dibagi menjadi kategori berdasarkan fungsi objek yang distandarisasi dalam proses produksi. Kategori ini termasuk standar produk, bahan baku, suku cadang, proses dan peralatan proses, standar pemeliharaan peralatan, standar metode inspeksi dan pengujian, standar teknis peralatan inspeksi, pengukuran dan pengujian, penanganan, penyimpanan, pengemasan, penandaan, dan sebagainya. Kelima, standar dapat dibagi menjadi standar manajemen, standar teknis, dan standar kerja berdasarkan karakteristiknya [9].

(2) Peraturan keamanan data Tiongkok Ada tiga standar keamanan informasi Tiongkok: standar keamanan informasi dasar, standar evaluasi keamanan teknologi informasi, dan standar manajemen keamanan informasi. Standar keamanan data dasar Kosa kata keamanan informasi, arsitektur keamanan informasi, kerangka kerja keamanan informasi, dan model keamanan informasi adalah standar dasar keamanan informasi. Kosakata Teknologi Informasi, Bagian 8: Keamanan (GB/T 5271.8-2001) menetapkan standar untuk kata-kata yang berkaitan dengan keamanan informasi. Model Referensi Dasar Interkoneksi Sistem Terbuka Sistem Pengolahan Informasi, Bagian 2, mencakup standar arsitektur keamanan informasi. Konstruksi Keamanan (GB/T 9387.2-1995) "Interkoneksi Sistem Terbuka Teknologi Informasi dan Kerangka Kerja Keamanan Sistem Terbuka" (GB/T 18794) adalah standar untuk kerangka kerja keamanan informasi. Standar untuk model keamanan informasi termasuk Model Keamanan Tinggi Interkoneksi Sistem Terbuka Teknologi Informasi (GB/T 17965-2000), Umum Bagian 1: Gambaran Umum, Model, dan Metode (GB/T 18237.1-2000), dan lainnya. Standar penilaian keamanan teknologi informasi: Ide perlindungan hierarkis pertama kali diusulkan oleh Trusted Computer System Evaluation Criteria (TCSEC). Ini merupakan dasar untuk standar penilaian keamanan teknologi informasi. Standar ini membagi keamanan sistem informasi komputer ke dalam empat kategori dan tujuh tingkatan: D, C1, C2, B1, B2, B3, dan A1. TCSEC kemudian diambil dan dikembangkan oleh Pedoman Evaluasi Produk Komputer Tepercaya Kanada (CTCPEC), Kriteria Federal AS (FC), dan Kriteria Evaluasi Keamanan Teknologi Informasi (ITSEC). Pedoman Klasifikasi Perlindungan Keamanan Sistem Informasi Komputer China (GB 17859-1999) pada tahun 1999 mengadopsi persyaratan TCSEC tingkat C1 hingga B3. Pedoman ini membagi keamanan sistem informasi komputer menjadi lima tingkat, yang

merupakan dasar sistem perlindungan tingkat keamanan informasi China. Kriteria Umum Evaluasi Keamanan Teknis Informasi (CCITSE atau CC) yang dibuat pada tahun 1999 didasarkan pada CC2. 1 standar yang diterbitkan oleh "Pedoman Penilaian Keamanan Teknologi Informasi Teknologi Keamanan Teknologi Informasi" (ISO / IEC 15408). China kemudian mengubah CC menjadi standar nasional yang disarankan, "Pedoman Evaluasi Keamanan Teknologi Informasi Teknologi Keamanan Teknologi Informasi" (GB/ 18336) setelah menjadi standar yang paling komprehensif saat ini untuk penilaian keamanan teknologi informasi. Standar manajemen keamanan informasi: Standar nasional untuk manajemen keamanan informasi terutama terdiri dari standar dan pedoman untuk keamanan informasi yang dibuat oleh American Institute of Standards and Technology (NIST SP800) dan standar untuk manajemen keamanan informasi yang dibuat oleh British Standards Association (seri BS 7799). Konvensi internasional yang berkaitan dengan sistem manajemen keamanan informasi (ISMS) termasuk "Kode Implementasi Manajemen Keamanan Informasi Teknologi Teknologi Informasi" (ISO/IEC 17799-2005), "Panduan Manajemen Keamanan Informasi Teknologi Informasi Panduan Manajemen Keamanan Jaringan" (BS ISO/IEC TR 13335-5-2001), dan lainnya. Organisasi Internasional untuk Standarisasi telah mencadangkan 60 nomor standar untuk ISMS, mulai dari ISO/IEC 27000 hingga ISO/IEC 27059. ISO/IEC 27000, yang berjudul "Sistem Manajemen Keamanan Informasi Teknologi Informasi, Tinjauan Umum dan Kosakata", memberikan definisi umum dan definisi dasar. prinsip yang terkandung dalam standar ISMS, yang merupakan standar paling dasar dalam kategori standar yang berkaitan dengan ISMS.

(3) Sistem standar Tiongkok untuk melindungi tingkat keamanan informasi. Di China, sistem perlindungan tingkat keamanan informasi adalah sistem, strategi, dan teknik utama untuk jaminan keamanan informasi. Peraturan Republik Rakyat Tiongkok tentang Perlindungan Keamanan Sistem Informasi Komputer, yang dikeluarkan pada tahun 1994 oleh Dewan Negara (Perintah 147 Dewan Negara), menunjukkan bahwa keamanan sistem informasi komputer telah ditingkatkan pada tahun 2011. Untuk melindungi tingkat keamanan informasi yang berbeda, sistem yang memiliki tingkat keamanan yang berbeda harus memiliki kemampuan yang berbeda. Menurut Pendapat Implementasi tentang Perlindungan Rahasia Keamanan Informasi, perlindungan rahasia keamanan informasi mengacu pada perlindungan keamanan hirarkis informasi rahasia negara, informasi hak milik dan publik dari badan hukum, organisasi, dan warga negara lain; sistem informasi yang menyimpan, mengirim, dan memproses informasi ini; manajemen produk keamanan informasi yang digunakan dalam sistem informasi; dan tanggapan hirarkis dan pemangku kepentingan terhadap produk keamanan informasi yang

digunakan dalam sistem informasi. Kementerian Keamanan Publik dan departemen standardisasi telah membentuk sistem standar untuk perlindungan tingkat keamanan informasi dengan bantuan departemen terkait, perusahaan, dan akademisi. Sistem ekonomi dan perdagangan (seperti perdagangan komersial, bea cukai, dll.); sistem keuangan (seperti keuangan, pajak, industri, dan perdagangan, dll.); sistem keuangan (seperti perbankan, asuransi, sekuritas, dll.); sistem informasi komputer untuk situs web utama dan akses publik ke Internet; sistem partai dan pemerintahan; sistem telekomunikasi (seperti pos dan telekomunikasi, telepon, dan internet); dan sistem telekomunikasi lainnya. Saat ini, standar dasar, standar aplikasi, standar produk, dan standar tambahan termasuk dalam empat kategori utama standar yang berkaitan dengan perlindungan tingkat keamanan informasi. Standar dasar untuk kelas: Standar dasar seperti Pedoman Klasifikasi Komputer Sistem Informasi Keamanan (GB 17859-1999).

Standar kelas aplikasi: "Panduan Klasifikasi Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi" (GB/T 22240-2020) adalah standar penilaian perlindungan keamanan informasi yang relevan untuk standar kelas aplikasi. Panduan Penerapan Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 25058-2019) adalah standar yang relevan untuk menerapkan perlindungan tingkat keamanan informasi. Keamanan Jaringan Teknologi Keamanan Informasi adalah standar untuk persyaratan perlindungan tingkat keamanan informasi.

Persyaratan dasar untuk perlindungan tingkat (GB/T 22239-2019), Persyaratan Teknis Keamanan Umum Sistem Informasi Teknologi Keamanan Informasi (GB/T 20271-2006), Persyaratan Teknis Desain Keamanan Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 25070- 2019), Persyaratan Manajemen Keamanan Sistem Informasi Teknologi Keamanan Informasi (GB/T 20269-2006), Persyaratan Teknis Teknologi Keamanan Informasi untuk Keamanan Dasar Jaringan Dasar (GB/T 20270- 200 Persyaratan Penilaian Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 28448-2019), Panduan Proses Evaluasi Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 28449-2018), dan Evaluasi Manajemen Keamanan Sistem Informasi Teknologi Keamanan Informasi (GA/T 713-2007) adalah beberapa standar yang berkaitan dengan evaluasi tingkat keamanan informasi.

Standar produk: Persyaratan teknis keamanan teknologi keamanan informasi sistem operasi (GB/T 20272-2019) dan kriteria penilaian keamanan teknologi keamanan informasi sistem operasi (GB/T 20008-2005) merupakan standar keamanan sistem operasi. Peraturan basis data yang relevan termasuk pedoman penilaian keamanan sistem manajemen basis data

teknologi keamanan informasi (GB/T 20009-2019), persyaratan teknis untuk keamanan sistem manajemen basis data teknologi keamanan informasi (GB/T 20273-2019), dan lainnya. Persyaratan teknis untuk keamanan jaringan teknologi keamanan informasi termasuk persyaratan teknis untuk keamanan produk jaringan dan produk isolasi terminal (GB / T 20279-2015), persyaratan teknis untuk keamanan produk pemindaian kerentanan jaringan teknologi keamanan informasi (GB / T 20278-2013), dan persyaratan teknis untuk keamanan sakelar jaringan (GB / T 21050-2019).

Standar kelas tambahan: Persyaratan untuk penilaian risiko yang relevan termasuk Teknologi Keamanan Informasi dan Kode Penilaian Risiko Keamanan Informasi (GB/T 20984-2007). Panduan Manajemen Kejadian Keamanan Informasi Teknologi Keamanan Informasi (GB/T 20985), Panduan Klasifikasi Kejadian Keamanan Informasi Teknologi Keamanan Informasi (GB/Z 20986-2007), dan Kode Pemulihan Bencana Sistem Informasi Teknologi Keamanan Informasi (GB/T 20988-2007) adalah peraturan yang relevan untuk manajemen kejadian keamanan informasi.

(4) Tahap perkembangan perlindungan tingkat keamanan informasi di Cina telah melewati tahap perlindungan level 1.0 dan 2.0. Perlindungan Tingkat 1.0: Peraturan Republik Rakyat Tiongkok tentang Perlindungan Keamanan Sistem Informasi Komputer, yang dikeluarkan oleh Dewan Negara pada tahun 1994, memberikan dasar untuk perlindungan tingkat keamanan informasi Tiongkok. China juga telah membuat standar teknis untuk menjamin perlindungan tingkat keamanan data. Dalam hal keamanan sistem informasi, kategori Panduan Klasifikasi Perlindungan Sistem Informasi Komputer (GB 17859-1999) membagi keamanan informasi China menjadi lima kategori. Tingkat perlindungan independen pengguna adalah tingkat pertama. Fitur keamanan melindungi data pengguna dari pencemaran yang tidak sah. Perlindungan audit sistem berada di tingkat kedua. Selain memiliki semua fitur keamanan Level 1, level ini juga memerlukan pembuatan dan pemeliharaan catatan pelacakan audit yang dapat diakses, yang membuat setiap pengguna bertanggung jawab atas legalitas tindakan mereka. Yang ketiga, tanda pengaman memiliki tingkat perlindungan yang sangat tinggi. Selain mempertahankan fungsi keamanan level sebelumnya, level ini mengharuskan pengunjung membatasi akses mereka sesuai dengan tingkat keamanan tanda objek akses, yang memungkinkan perlindungan objek akses yang diperlukan. Tingkat keempat terdiri dari perlindungan terstruktur. Untuk meningkatkan resistensi terhadap penetrasi sistem, tingkat ini mewarisi tingkat fungsi keamanan di atas dan membaginya menjadi bagian kunci dan non-kunci. Tingkat kelima melindungi verifikasi akses. Dalam tingkat ini, otentikasi akses ditambahkan untuk mengesahkan semua aktivitas akses pengunjung. Selain itu, "Langkah-

langkah manajemen perlindungan tingkat keamanan informasi" membagi sistem informasi menjadi lima tingkat keamanan, dimulai dengan tingkat keamanan rendah dan berakhir pada tingkat kerusakan pada negara, tatanan sosial, badan hukum, dan organisasi lain. Dalam hal manajemen dan pengawasan sistem informasi.

Langkah-langkah untuk Manajemen Perlindungan Tingkat Keamanan Informasi menetapkan bahwa unit operasi dan pengguna sistem informasi harus melindungi sistem informasi sesuai dengan langkah-langkah dan standar teknis yang relevan. Selain itu, departemen pengawasan dan administrasi keamanan informasi negara yang relevan harus mengawasi dan mengelola pekerjaan yang berkaitan dengan perlindungan tingkat keamanan informasi. Pengguna sistem informasi harus mematuhi "Persyaratan Dasar Perlindungan Tingkat Keamanan Sistem Informasi Teknologi Keamanan Informasi" (GB / T 22239-2008, telah diganti) untuk meningkatkan pekerjaan perlindungan tingkat keamanan informasi, mematuhi teknologi, mengembangkan secara terkoordinasi, dan mematuhi manajemen paralel ganda. Dalam teknologi, tingkat keamanan informasi diperbaiki dalam lima bagian: keamanan fisik, keamanan host, keamanan aplikasi, keamanan jaringan, dan pencadangan dan pemulihan data. Dalam manajemen, tingkat keamanan informasi diperbaiki dalam lima bagian: personel keamanan, organisasi manajemen keamanan, sistem manajemen keamanan, manajemen konstruksi dan operasi sistem, dan manajemen pemeliharaan. Sesuai dengan prosedur yang telah ditetapkan, lembaga evaluasi akan melakukan evaluasi tingkat sistem informasi. Laporan evaluasi membantu personel manajemen sistem informasi memahami apakah sistem informasi memiliki perlindungan keamanan yang tepat dan memenuhi persyaratan keamanan yang relevan. keahlian. Unit pencatatan harus, sesuai dengan persyaratan, secara teratur memeriksa pelaksanaan pekerjaan perlindungan tingkat keamanan informasi; memiliki pengetahuan tentang indikator teknis dan manajemen keamanan sistem informasi yang relevan; dan mengambil tindakan teknis dan manajemen yang ditargetkan untuk mengidentifikasi bahaya keamanan tersembunyi yang ada dalam sistem informasi.

Pada saat ini, persyaratan teknis untuk perlindungan tingkat keamanan sistem informasi termasuk Panduan Penilaian Perlindungan Tingkat Keamanan Sistem Informasi (GB/T 22240-2008), Panduan Penerapan Perlindungan Tingkat Keamanan Sistem Informasi (GB/T 25058-2010), Persyaratan Teknis Desain Perlindungan Tingkat Keamanan Sistem Informasi (GB/T 25070-2010), Persyaratan Penilaian Perlindungan Tingkat Keamanan Sistem Informasi (GB/T 28448-2012), dan Panduan Proses Penilaian Perlinduan Saat ini, standar teknis ini telah diganti. Tahap Perlindungan Tingkat 2.0: Tiongkok membuat dan merevisi serangkaian standar terkait pada tanggal 1 Juni 2017, setelah undang-undang keamanan jaringan Republik Rakyat

Tiongkok. Ini dilakukan untuk bekerja sama dengan penerapan undang-undang ini, serta dengan teknologi baru seperti komputasi awan, data besar, Internet of Things, dan lainnya, untuk membuat aplikasi baru yang melindungi tingkat keamanan informasi dari perubahan dan persyaratan baru. Persyaratan Dasar Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB / T 22239-2019), Panduan Implementasi Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB / T 25058-2019), Panduan Klasifikasi Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB / T 22240- 2020), Persyaratan Teknis Desain Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB / T 25070-2019), dan Persyaratan Penilaian Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi telah dikompilasi / direvisi dan diterbitkan (GB / T 28448-2019), Panduan Proses Penilaian Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 28449-2018), Panduan Teknis Pengujian dan Evaluasi Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 36627-2018), Persyaratan Teknis Pusat Manajemen Keamanan Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 36958- 2018), Spesifikasi Badan Penilaian Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB/T 36959-2018), dan lain-lain. Jika dibandingkan dengan GB/T 22239-2008, tahap perlindungan 1.0, GB / T 22239-2019 mengubah nama standar, tingkat objek perlindungan, persyaratan keamanan, klasifikasi keamanan, pusat manajemen keamanan, verifikasi tepercaya, dan informasi lainnya. Nama standar yang baru diubah menjadi "Persyaratan dasar perlindungan tingkat keamanan jaringan teknologi keamanan informasi". Standar ini memperluas objek perlindungan tingkat dari sistem informasi asli ke jaringan informasi dasar, platform/sistem komputasi awan, aplikasi/platform/sumber daya data besar, sistem Internet of Things, sistem kontrol uji coba industri, dll. Sistem manajemen keselamatan, organisasi manajemen keselamatan, manajemen personel keselamatan, manajemen konstruksi keselamatan, manajemen operasi dan pemeliharaan keselamatan, dll. adalah jenis persyaratan manajemen yang berbeda. Persyaratan keselamatan level 2 ke atas kini mencakup "pusat manajemen keselamatan".

Dalam persyaratan keselamatan tersier dan di atas, pusat manajemen keselamatan telah menambahkan "manajemen sistem" dan "manajemen audit" sebagai elemen konten; di pusat manajemen keselamatan sekunder, ini telah menambahkan "manajemen sistem", "manajemen audit", "manajemen keselamatan", "kontrol terpusat", dan elemen lainnya. "Jaringan komunikasi yang aman", "batas area yang aman", dan "lingkungan komputasi yang aman" semuanya mengandung kata "verifikasi tepercaya" dalam hal verifikasi tepercaya.

Secara umum, perlindungan tingkat 2.0 meningkatkan jangkauan objek. Perlindungan tingkat keamanan data yang lebih tinggi, peningkatan teknik untuk melindungi tingkat keamanan data yang lebih tinggi, dan penambahan standar teknis yang relevan. Didasarkan pada undang-undang Republik Rakyat Tiongkok tentang peraturan perlindungan keamanan sistem informasi komputer, tahap perlindungan tingkat 1.0 dan tahap perlindungan tingkat 2.0 berasal dari undang-undang keamanan jaringan Republik Rakyat Tiongkok, yang meningkatkan tahap perlindungan tingkat 1.0 dari "sistem perlindungan tingkat keamanan informasi" menjadi "sistem perlindungan tingkat keamanan jaringan." Tidak memberikan perlindungan hierarkis melanggar Undang-Undang Keamanan Siber Republik Rakyat Tiongkok, dan akan dihukum sesuai dengan ketentuan hukum yang relevan.

(5) Persyaratan yang berkaitan dengan keamanan data perdagangan elektronik "Panduan Konstruksi Keamanan Informasi Teknologi Keamanan Informasi Perusahaan E-commerce Kecil dan Menengah" (GB/Z 32906-2016), "Operasi Platform E-commerce dan Spesifikasi Teknis" (GB/T 31524-2015), dan lain-lain adalah standar untuk keamanan informasi e-commerce.

4. **Undang-undang dan peraturan keamanan informasi**

Konvensi hukum adalah aturan yang ditetapkan atau disetujui oleh badan legislatif sebuah negara untuk mengarahkan dan mengontrol perilaku seseorang. Karakteristik substantif dari norma hukum adalah sebagai berikut: Pertama, norma hukum adalah norma yang ditetapkan atau diakui oleh negara dan dijamin oleh kekuatan negara, sehingga memiliki karakteristik kehendak dan kekuasaan negara. Kedua, norma hukum didasarkan pada penetapan kekuasaan hukum dan kewajiban hukum, yang merupakan kode etik khusus dengan struktur logis yang lengkap. Ketiga, norma hukum secara umum mengikat, dan norma-norma ini akan memandu dan menentukan apa yang harus dilakukan. Oleh karena itu, hukum yang ditetapkan oleh negara berlaku untuk semua warga negara Tiongkok, dan siapa pun wajib mematuhinya. Hukum dan norma keamanan informasi adalah istilah yang mengacu pada semua peraturan dan peraturan yang berkaitan dengan keamanan data. Norma imperatif dan norma larangan adalah dua kategori utama. Standar imperatif menetapkan bahwa subjek hubungan hukum, termasuk warga negara, individu, lembaga, dan negara, harus melakukan tindakan tertentu; jika mereka tidak melakukannya, mereka akan dikenakan sanksi.

(1) Struktur sistem hukum keamanan informasi Tiongkok Terdiri dari empat tingkat: undang-undang, peraturan administratif, dokumen dan peraturan normatif, dan peraturan lokal. Hukum Tiongkok yang terkait dengan keamanan informasi terutama mencakup Hukum Keamanan Negara Republik Rakyat Tiongkok, hukum Republik Rakyat Tiongkok tentang Menjaga

Rahasia Negara, hukum tanggung jawab hukum Republik Rakyat Tiongkok, hukum pertanggungjawaban gugatan Republik Rakyat Tiongkok, hukum tanda tangan elektronik Republik Rakyat Tiongkok, keputusan Komite Tetap Kongres Rakyat Nasional untuk menjaga keamanan Internet, hukum keamanan jaringan Republik Rakyat Tiongkok, hukum perdagangan elektronik Republik Rakyat Tiongkok, hukum kata sandi Republik Rakyat Tiongkok, dll. Peraturan administratif yang terkait dengan keamanan informasi terutama mencakup peraturan Republik Rakyat Tiongkok tentang perlindungan keamanan sistem informasi komputer, Ketentuan Sementara Republik Rakyat Tiongkok tentang administrasi jaringan internasional jaringan informasi komputer, langkah-langkah administratif untuk perlindungan keamanan jaringan internasional jaringan informasi komputer, peraturan tentang administrasi kata sandi komersial, Peraturan Telekomunikasi Republik Rakyat Tiongkok Langkah-langkah untuk administrasi layanan informasi Internet, peraturan tentang administrasi tempat bisnis layanan Internet, peraturan tentang perlindungan perangkat lunak komputer, peraturan tentang komunikasi jaringan informasi, dll. Dokumen normatif, yang biasanya disebut sebagai "dokumen berkepala merah", dibuat oleh komisi, kementerian, Bank Rakyat Tiongkok, Kantor Audit Nasional, dan lembaga lain yang berada langsung di bawah Dewan Negara dengan fungsi administratif (selanjutnya disebut "departemen Dewan Negara") sesuai dengan undang-undang dan peraturan administratif Dewan Negara. Peraturan daerah dibuat oleh badan-badan kekuasaan negara di tingkat daerah sesuai dengan kewenangan mereka dan dengan asumsi bahwa ada perbedaan antara konstitusi, undang-undang, dan peraturan administratif. Perjanjian internasional juga disebut sebagai konvensi, kesepakatan, perjanjian, kontrak, deklarasi, dll., dan dibuat antara subjek hukum internasional dengan menggunakan hukum internasional sebagai norma dan menetapkan kekuasaan dan kewajiban timbal balik. Interpretasi yudisial mengacu pada interpretasi yang diberikan oleh organ yudisial tertinggi negara tentang penerapan hukum, khususnya dalam proses penerapan hukum.

(2) Pengenalan undang-undang dan undang-undang yang relevan: Berikut ini terutama memperkenalkan "Peraturan Republik Rakyat Tiongkok tentang Perlindungan Keamanan Sistem Informasi Komputer" dan "Hukum Tanda Tangan Elektronik Republik Rakyat Tiongkok". Peraturan ini pertama kali dikeluarkan pada tanggal 18 Februari 1994, dan terakhir kali direvisi pada tahun 2011. Pertama dan terpenting, tujuan dan status hukum. Tujuan peraturan ini adalah untuk mendorong pengembangan dan aplikasi komputer serta menjaga sistem informasi komputer aman. Peraturan ini tidak hanya merupakan peraturan paling awal tentang perlindungan keamanan sistem informasi China, tetapi juga peraturan paling dasar. Ini menetapkan dasar untuk hukum dan peraturan yang relevan di masa depan tentang

perlindungan keamanan sistem informasi China. Sejak saat itu, China telah membuat sistem hukum yang cukup lengkap untuk keamanan informasi dengan memberlakukan berbagai undang-undang dan peraturan tentang keamanan informasi, termasuk undang-undang untuk mencegah dan mengendalikan virus komputer, undang-undang untuk keamanan jaringan informasi komputer dan jaringan antar negara, dan undang-undang untuk layanan informasi Internet. Kedua, luasnya penerapan. Pasal 5 menetapkan bahwa objek perlindungan peraturan adalah sistem informasi komputer di seluruh Republik Rakyat Tiongkok, dan Pasal 7 menetapkan bahwa organisasi atau individu adalah kelompok yang dapat diterapkan dari peraturan. Sehubungan dengan keamanan komputer mikro non-jaringan, peraturan ini tidak berlaku. Pasal 29 menetapkan bahwa keamanan sistem informasi komputer tentara harus dilakukan sesuai dengan hukum dan peraturan tentara yang relevan. Ketiga, topik utama Terutama, peraturan tersebut mencakup persyaratan umum, sistem keamanan, pengawasan keamanan, tanggung jawab hukum, dan persyaratan tambahan, antara lain.

Tabel 4.3 Peraturan dan dokumen normatif yang terkait dengan keamanan informasi

Aturan Sektor dan Dokumen Normatif	Isi Peraturan
Kementerian Keamanan Publik	- Proses administratif untuk inspeksi dan lisensi penjualan produk khusus guna menjamin keamanan sistem informasi komputer. - Langkah-langkah perlindungan keamanan dan manajemen jaringan informasi internasional. - Regulasi teknis terkait perlindungan keamanan internet. - Kebijakan administratif untuk pencegahan dan pengendalian virus komputer.
Kementerian Keamanan Publik, Bank Rakyat Tiongkok	- Regulasi sementara terkait perlindungan keamanan sistem informasi komputer di lembaga keuangan.
Kementerian Perindustrian dan Teknologi Informasi	- Aturan administratif mengenai layanan pengumuman elektronik di internet. - Panduan manajemen produk perangkat lunak. - Regulasi administratif untuk

	pengelolaan biro masuk komunikasi internasional. - Ketentuan terkait administrasi pembangunan infrastruktur komunikasi internasional. - Pedoman manajemen nama domain pada jaringan internet. - Kebijakan sementara untuk pengelolaan jaringan telekomunikasi publik. - Aturan administratif mengenai layanan sertifikasi elektronik. - Langkah-langkah administratif untuk menjaga keamanan komunikasi jaringan.
Kantor Informasi Dewan Negara & Kementerian Teknologi Informasi	- Regulasi sementara terkait pengelolaan bisnis penerbitan berita di stasiun internet.
Kementerian Pendidikan	- Kebijakan administratif sementara untuk jaringan komputer pendidikan dan penelitian ilmiah di Tiongkok. - Regulasi administratif sementara untuk situs web pendidikan dan sekolah daring.
Berita Nasional & Administrasi Umum	- Kebijakan administratif mengenai publikasi elektronik.
Biro Rahasia Perlindungan Nasional	- Regulasi sementara tentang manajemen kerahasiaan sistem informasi komputer.
Administrasi Kriptografi Nasional	- Peraturan terkait produksi dan pengelolaan produk sandi komersial.
Komisi Regulasi Sekuritas China	- Kebijakan administratif terkait regulasi layanan sekuritas secara daring.
Administrasi Produk Medis Nasional	- Panduan administratif mengenai pemberian layanan informasi obat di internet.
Lainnya	- Regulasi terkait manajemen kerahasiaan jaringan informasi

	internasional. - Ketentuan sementara terkait pemeriksaan dan persetujuan komunikasi, otomasi kantor, serta sistem informasi komputer mengenai kata sandi nasional. - Prosedur administratif terkait integrasi sistem informasi rahasia.

(1) Memberikan definisi dari istilah "sistem informasi komputer". Dalam peraturan ini, istilah "sistem informasi komputer" mengacu pada sistem manusia-komputer-mesin yang terdiri dari komputer, peralatan, fasilitas, dan pendukungnya, serta jaringan yang mengumpulkan, memproses, menyimpan, mengirimkan, dan mengambil data untuk tujuan dan aplikasi tertentu.

(2) Ada penjelasan yang jelas tentang karakteristik dan fungsi penting dari keamanan sistem informasi komputer untuk pekerjaan perlindungan.

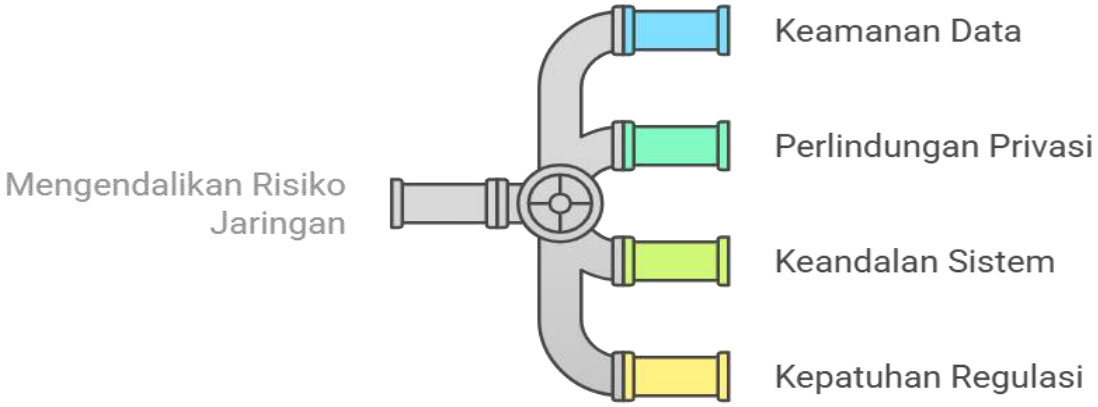
(3) Sistem perlindungan keamanan: Pasal 9 mengatur sistem perlindungan tingkat keamanan, Pasal 10 mengatur sistem perlindungan keamanan ruang komputer, Pasal 11 mengatur sistem pencatatan jaringan internasional, Pasal 12 mengatur pernyataan masuk dan keluar dari sistem media informasi, Pasal 13 mengatur sistem tanggung jawab manajemen keamanan informasi komputer, Pasal 14 mengatur sistem laporan kejahatan, dan Pasal 15 mengatur sistem pencegahan pemalsuan informasi.

4) Wewenang dan kewajiban pengawasan keselamatan: Pasal 6, 17, 18, dan 19 dengan jelas menetapkan bahwa Kementerian Keamanan Publik bertanggung jawab untuk menjaga keamanan sistem informasi komputer nasional, dan Pasal 17, 18, dan 19 dengan jelas menetapkan wewenang dan kewajiban untuk mengawasi organ keamanan publik.

5) Tanggung jawab hukum pelaku: Pasal 20 sampai 25 dan 27 mengatur tanggung jawab hukum pelaku dan hukuman. 6) Mendefinisikan virus komputer dan produk keamanan khusus: Pasal 28 mengatur produk keamanan khusus untuk virus komputer dan keamanan sistem informasi komputer. Hukum Tanda Tangan Elektronik Republik Rakyat Tiongkok (juga dikenal sebagai Hukum Tanda Tangan Elektronik) diberlakukan pada tanggal 1 April 2005. Versi saat ini dirilis pada April 2019. Tentukan tujuan Anda terlebih dahulu. Tujuan dari Undang-Undang Tanda Tangan Elektronik dijelaskan dalam Pasal 1 undang-undang tersebut. Tujuannya adalah untuk mengatur cara orang menggunakan tanda tangan elektronik, menetapkan efeknya, dan melindungi hak dan kepentingan yang sah dari semua pihak yang

terkait. Kedua, lihat definisi undang-undang tanda tangan elektronik. Pasal 2 mendefinisikan tanda tangan elektronik sebagai data yang dilampirkan dalam bentuk elektronik untuk mengidentifikasi identitas penandatangan dan menunjukkan bahwa mereka mengakui isi. Informasi yang dibuat, dikirim, diterima, atau disimpan dengan cara elektronik, optikal, magnetik, atau cara serupa disebut sebagai data "sebagaimana digunakan dalam Undang-Undang ini". Dalam Undang-Undang Tanda Tangan Elektronik, Pasal 34 menjelaskan definisi istilah yang terkait. Di antaranya, penandatangan elektronik mengacu pada orang yang memegang data yang digunakan untuk membuat tanda tangan elektronik dan menggunakannya atas namanya sendiri atau atas nama orang yang diwakilinya. Orang yang terlibat dalam kegiatan yang relevan berdasarkan kepercayaan sertifikat sertifikasi tanda tangan elektronik atau tanda tangan elektronik disebut sebagai pihak yang bergantung pada tanda tangan elektronik. Sertifikasi sertifikasi tanda tangan elektronik adalah pesan data atau catatan elektronik lainnya yang dapat mengkonfirmasi bahwa penandatangan elektronik terhubung dengan data produksi tanda tangan elektronik. Data produksi tanda tangan elektronik mencakup karakter, kode, dan data lainnya yang digunakan dalam proses tanda tangan elektronik untuk menghubungkan orang yang menandatangani tanda tangan elektronik secara andal dengan mereka. Ketiga, luasnya aplikasi. Ruang lingkup instrumen yang dapat dan tidak dapat digunakan oleh Undang-Undang ini diatur dalam Pasal 3 dan 35. Keempat, konsekuensi hukum dari Undang-Undang Tanda Tangan Elektronik: Pasal 4 hingga 12 membahas efek hukum dari pesan data, dan Pasal 13 hingga 15 membahas konsekuensi hukum dari tanda tangan elektronik. Kelima, sertifikasi tanda tangan elektronik Pasal 16-26 UU ini menetapkan persyaratan, proses permohonan, dan layanan sertifikasi, serta ketentuan terkait untuk penyediaan layanan sertifikasi tanda tangan elektronik. Keenam, tanggung jawab hukum: Pasal 27 hingga 33 UU ini mengatur tanggung jawab hukum yang terkait dengan pelanggaran terhadap UU ini.

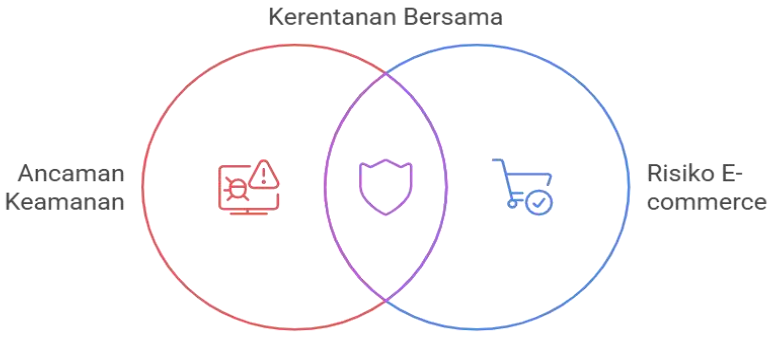
BAB 5
Mengendalikan Risiko Jaringan dalam *E-Commerce*



Gambar 5.1 Menavigasi Risiko Jaringan dalam E-commerce

Internet secara alami rentan terhadap keamanan informasi karena sifatnya yang terbuka dan terbuka. Selain itu, serangan baru terhadap kerentanan protokol jaringan dan aplikasi muncul di seluruh dunia, terutama karena adanya kecerdasan dan otomatisasi serangan jaringan. Tindakan pencegahan dan respons yang cepat diperlukan karena kebocoran atau kehilangan data dapat melanggar hak privasi konsumen dan bahkan berpotensi merugikan bisnis, lembaga penelitian, dan pemerintah.

5.1 Ancaman Keamanan Jaringan E-commerce dan Identifikasi Risiko



Gambar 5.2 Ancaman dan Risiko Keamanan E-commerce

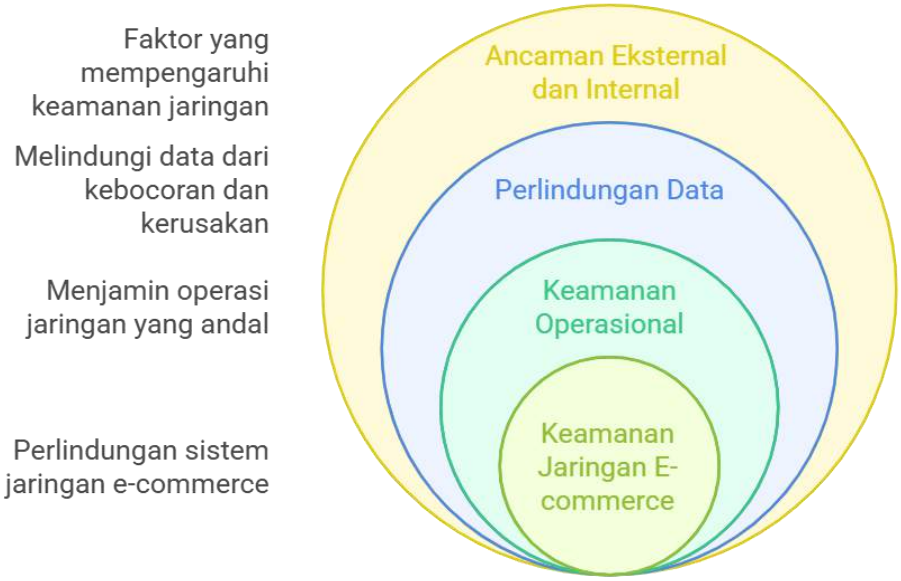
Untuk menjalankan e-commerce, internet dan jaringan informasi lainnya adalah sarana; ini juga termasuk media dan lingkungan operasi dasar yang diperlukan untuk menjalankannya. Ini adalah bagian penting dari manajemen keamanan e-commerce karena keamanan berdampak langsung pada keamanan e-commerce. Keamanan jaringan e-commerce mengacu pada operasi normal sistem jaringan e-commerce yang berkelanjutan dan dapat diandalkan dengan

mengadopsi berbagai langkah untuk melindungi perangkat keras, perangkat lunak, dan data sistem jaringan e-commerce dari kerusakan, perubahan, dan kebocoran oleh faktor alam dan buatan manusia serta faktor berbahaya lainnya. Keamanan jaringan e-commerce adalah bagian dari keamanan jaringan, dan termasuk keamanan operasional sistem jaringan e-commerce.

5.1.1 Ancaman Keamanan terhadap Jaringan E-commerce

Beberapa ancaman terhadap keamanan jaringan e-commerce dirangkum di bawah ini.

1. Risiko keamanan terhadap informasi jaringan e-commerce



Gambar 5.3 Hierarki Keamanan E-commerce

Ini adalah ancaman utama yang memicu masalah keamanan e-commerce. Ini adalah risiko yang dihadapi informasi jaringan e-commerce. Berbagai tingkatan, seperti sistem operasi, database, aplikasi, dan jaringan, termasuk risiko keamanan yang sangat sering terjadi dan berdampak besar pada keamanan sistem e-commerce. Penyalahgunaan atau ultra vires, peniruan data, kebocoran data, perusakan data, risiko penolakan, pencurian data, kode berbahaya, serangan jaringan, dll.

Risiko keamanan tersebut termasuk penggunaan peralatan yang tidak sesuai, perangkat lunak yang dipalsukan, akses yang tidak sah ke sumber daya sistem dan jaringan, penyalahgunaan izin untuk mengubah konfigurasi sistem, atau melampaui batas atau penyalahgunaan.

Peniruan informasi adalah peniruan atau pencurian akun dan otentikasi palsu untuk tujuan membuat informasi palsu dan merusak informasi yang sebenarnya.

Kebocoran informasi termasuk kebocoran informasi internal dan eksternal. Sebagian besar, bahaya keamanan seperti itu berasal dari tindakan manusia yang disengaja atau tidak disengaja. Sebagai contoh, penyusup dapat memperoleh informasi melalui tindakan yang melanggar hukum, seperti pengintaian jarak jauh, intersepsi sinyal, penyadapan, pencurian media atau file, pencurian perangkat, dan mendaur ulang atau membuang media. Informasi seperti akun pengguna dan kata sandi dapat dengan mudah disusupi.

Perkataan "perusakan informasi" mengacu pada perubahan informasi yang melanggar hukum, perusakan integritas informasi, dan membuat sistem tidak aman atau tidak dapat digunakan. Perusakan informasi konfigurasi jaringan, informasi konfigurasi sistem, informasi konfigurasi keamanan, informasi identitas pengguna, dan informasi bisnis adalah salah satu risiko keamanan tersebut. Penyebaran industri, aplikasi, dan layanan konvensional ke internet telah meningkatkan risiko perusakan data. Menurut Pusat Darurat Internet Nasional (CNCERT), jumlah situs web yang dirusak di China pada paruh pertama tahun 2020 meningkat dari 50.527 pada periode yang sama tahun sebelumnya.

Penyangkalan mengacu pada penyangkalan tindakan, transaksi, dan informasi yang dikirim dan diterima. Penyangkalan asal, penyangkalan penerimaan, dan penyangkalan pihak ketiga adalah contoh dari jenis bahaya keamanan ini.

Penyangkalan asal adalah ketika pengirim pesan menyangkal bahwa pesan telah dibuat dan dikirim, sedangkan penyangkalan penerimaan adalah ketika penerima pesan menyangkal memiliki menerima pesan tersebut. Karena penyangkalan dapat terjadi sebelum, saat, dan sesudah transaksi, ini adalah persyaratan penting dalam e-commerce.

Sebagai contoh, penelitian ilmiah memastikan bahwa orang yang benar tidak dapat menyangkal bahwa mereka membuat dan mengirim pesan tertentu untuk mencegah penyangkalan asli. Misalkan perusahaan A membuat dan mengirimkan pesanan ke perusahaan B. Setelah perusahaan B memproses pesanan dan mengeluarkan wesel, perusahaan A tidak dapat membantah bahwa ia telah mengirimkannya.

Teknik otentikasi dan tanda tangan digital adalah cara utama untuk mencegah penyangkalan. Penggunaan kerentanan, pintu belakang, atau saluran tersembunyi untuk meretas sistem jaringan orang lain untuk mencuri data atau informasi rahasia, dll. dikenal sebagai pencurian informasi.

Virus, bom logika, Trojan horse, worm, pintu jebakan, spyware, perangkat lunak penyadap, dan lainnya adalah contoh kode program yang dengan sengaja melakukan tugas-tugas berbahaya pada sistem komputer.

2. Risiko keamanan terhadap komunikasi jaringan e-commerce

Serangan jaringan merupakan sumber utama ancaman keamanan untuk komunikasi jaringan e-commerce. Serangan jaringan adalah penyusupan dan serangan yang memanfaatkan kelemahan keamanan jaringan. Seorang penyerang dapat melancarkan serangan dari luar ke intranet perusahaan atau dari dalam melalui jaringan area lokal di mana dia berada, dengan mendapatkan akses yang tidak sah ke mesin di dalam perusahaan.

Pekerja dalam perusahaan juga dapat melakukan serangan jarak jauh semu, yaitu, untuk menyembunyikan identitas penyerang, mereka meluncurkan serangan ke target lokal dari jara.

Sehubungan dengan metode yang digunakan, serangan jaringan dapat diklasifikasikan menjadi serangan baca, serangan operasi, serangan spoofing, serangan banjir, serangan pengalihan, dan serangan Rootkit.

Serangan baca biasanya berasal dari pengintaian dan pemindaian, yang menghasilkan penolakan layanan. Serangan operasional menggunakan perusakan data untuk mengganggu fungsionalitas program yang berjalan dan mengambil kendali atas program. Contohnya termasuk injeksi SQL, yang menyuntikkan SQL (bahasa kueri terstruktur) ke dalam sistem manajemen basis data (DBMS) untuk mendapatkan akses, dan serangan buffer overflow, yang menulis ke buffer program lebih lama daripada kapasitasnya, menyebabkan buffer meluap, yang merusak tumpangnya. Serangan spoofing terjadi ketika seseorang menyamar sebagai entitas lain untuk melakukan serangan.

Salah satu contohnya adalah ketika seseorang menangkap urutan autentikasi dan kemudian memutar ulang urutan tersebut setelah urutan autentikasi yang sah dikirim. Dengan cara ini, penyerang dapat menyerang sistem jaringan dengan meniru entitas yang memiliki hak istimewa tertentu. ARP, DNS, Web, dan IP address spoofing adalah beberapa contoh serangan spoofing yang paling umum. Selain itu, phishing, sejenis serangan yang meyakinkan orang untuk mendapatkan akun dan kata sandi mereka melalui email atau dengan meniru URL situs web tertentu, juga termasuk dalam kategori serangan ini.

Sumber utama ancaman keamanan bagi komunikasi jaringan e-commerce adalah serangan jaringan, yang merupakan penyusupan dan serangan yang memanfaatkan kelemahan keamanan jaringan. Seorang penyerang dapat melakukan serangan ke intranet perusahaan dari luar atau dari dalam melalui jaringan area lokal tempat dia berada, dengan mendapatkan akses yang tidak sah ke mesin di dalam organisasi.

Selain itu, karyawan organisasi memiliki kemampuan untuk melakukan serangan jarak jauh semu yaitu, untuk menyembunyikan identitas penyerang, mereka meluncurkan serangan ke target lokal dari penjara. Serangan jaringan dapat dikategorikan menjadi serangan baca,

serangan operasi, serangan spoofing, serangan banjir, serangan pengalihan, dan serangan Rootkit, berdasarkan metode yang digunakan. Serangan baca biasanya berasal dari pengintaian dan pemindaian, yang menyebabkan penolakan layanan.

Serangan operasional menggunakan perusakan data untuk mengganggu operasi program dan mengambil kendali atas program. Contohnya termasuk injeksi SQL, yang memasukkan SQL (bahasa kueri terstruktur) ke dalam DBMS untuk mendapatkan akses, dan serangan buffer overflow, yang menulis ke buffer program lebih lama daripada kapasitasnya, menyebabkan buffer meluap, yang merusak tumpangnya.

Ketika seseorang menyamar sebagai orang lain untuk melakukan serangan, itu disebut serangan spoofing. Salah satu contohnya adalah ketika seseorang menangkap urutan autentikasi dan kemudian memutar ulangnya setelah urutan autentikasi yang sah dikirim. Dengan cara ini, pencuri dapat memasuki sistem jaringan dengan meniru entitas dengan hak istimewa tertentu. Serangan spoofing sangat umum, termasuk spoofing ARP, DNS, Web, dan IP address. Termasuk dalam kategori serangan ini juga phishing, sejenis serangan yang meyakinkan orang untuk mendapatkan akun dan kata sandi mereka melalui email atau dengan meniru URL situs web tertentu.

3. Risiko keamanan pada jaringan m-commerce.

M-commerce menghadapi masalah keamanan karena protokol jaringan, koneksi nirkabel, dan perangkat terminal seluler. Protokol jaringan mengatur dirinya sendiri (ad hoc) adalah jaringan yang terdiri dari perangkat nirkabel yang menghubungkan node seluler satu sama lain tanpa bergantung pada fasilitas jaringan tetap. Dengan demikian, penyerang dapat mengkompromikan node seluler yang bekerja sama berdasarkan hubungan kepercayaan yang diasumsikan.

Sebagian besar paket data dalam komunikasi seluler dikirim dalam bentuk plaintext atau dienkripsi dengan keamanan yang lemah, sehingga sangat mudah untuk disadap dan dibobol dalam hal tautan nirkabel. Karena penyebaran sinyal nirkabel dan mobilitas komunikasi seluler, lebih sulit untuk mengidentifikasi perilaku penyerang. Penggunaan layanan hotspot Wi-Fi gratis sangat berbahaya.

Penyerang dapat mengendus pengguna lain di jaringan dan mencegat informasi yang dikirimkan oleh pengguna melalui perangkat lunak profesional, seperti nama pengguna, kata sandi, catatan transaksi, catatan obrolan, dan konten email, setelah masuk ke jaringan Wi-Fi gratis. Selain itu, penyerang juga dapat dengan kejam merusak alamat server DNS router Wi-Fi, sehingga ketika pengguna mengunjungi situs web biasa, browser mereka diarahkan ke URL berbahaya dan ilegal, membuat mereka terpapar pada ancaman phishing dan virus situs web.

Perangkat seluler mudah hilang atau dicuri karena kecil, mudah digunakan, dan bernilai tinggi. Selain itu, virus dapat sangat berbahaya untuk perangkat seluler.

5.1.2 Identifikasi Risiko Keamanan Jaringan E-commerce

Identifikasi risiko keamanan jaringan e-commerce mencakup menentukan aset informasi jaringan yang harus dilindungi oleh perusahaan e-commerce, menentukan kerentanan yang ada pada aset informasi jaringan, dan menentukan semua potensi bahaya yang mereka hadapi, serta menentukan prosedur keamanan yang telah digunakan untuk melindungi objek fisik, dan menggunakan teknik tertentu untuk mengukur tingkat risiko yang dihadapi oleh objek yang dilindungi. Bagian-bagian berikut terutama mencakup identifikasi ancaman keamanan jaringan e-commerce.

Keamanan lingkungan fisik mencakup lokasi, kontrol akses, pencegahan pencurian dan perusakan, perlindungan terhadap petir, kebakaran, air, dan kelembapan, kontrol suhu, catu daya, perlindungan elektromagnetik, dan lainnya.

Domain keamanan jaringan mengacu pada subnet atau jaringan dalam sistem yang sama yang memiliki kebutuhan perlindungan keamanan yang sama, saling mempercayai, dan memiliki kebijakan kontrol akses keamanan dan kebijakan kontrol batas yang sama.

Bagian domain keamanan jaringan mencakup apakah jaringan dibagi menjadi beberapa domain keamanan independen, dan apakah ada isolasi fisik atau isolasi logis di antara domain keamanan, dll. Bagian arsitektur jaringan mencakup redundansi perangkat keras perangkat jaringan penting dan perangkat komputasi penting, bandwidth, jalur akses yang aman, dll. Bagian komunikasi jaringan mencakup keamanan, integritas, dan kerahasiaan transmisi komunikasi, verifikasi tepercaya (yang berarti verifikasi tepercaya dari bootloader sistem dan program sistem perangkat komunikasi berdasarkan root tepercaya, dan alarm setelah mendeteksi kepercayaan rusak), dll. Bagian batas area keamanan mencakup perlindungan batas, kontrol akses, pencegahan kode berbahaya, dll.

Apakah penyebaran peralatan deteksi lalu lintas jaringan memenuhi persyaratan yang relevan adalah bagian dari pencegahan intrusi.

Audit keamanan mencakup apakah sistem audit pihak ketiga disiapkan untuk mengaudit dan apakah server log khusus disiapkan untuk mengumpulkan dan menyimpan log peralatan jaringan.

Bagian perlindungan peralatan jaringan memeriksa apakah kontrol akses dan otentikasi yang digunakan untuk mengontrol peralatan jaringan dan akses ke server memenuhi persyaratan yang relevan.

Komponen pencadangan dan pemulihan memeriksa apakah konfigurasi jaringan dapat dicadangkan segera ke server pencadangan khusus ketika konfigurasi diubah, dan apakah konfigurasi sistem operasi dan peralatan jaringan memenuhi persyaratan yang relevan.

Di antara komponen sistem jaminan keamanan adalah deteksi kerentanan halaman web, pemantauan gangguan situs web dalam waktu nyata, serangan penolakan layanan yang terdistribusi, deteksi keamanan port, peringatan masuk di luar situs, pertahanan yang keras terhadap peretasan kata sandi host, deteksi pintu belakang situs web, dll.

Bagian manajemen rantai pasokan termasuk memastikan bahwa pemilihan pemasok memenuhi peraturan nasional yang berlaku, dan sebagainya. Dalam proses identifikasi risiko, pendekatan untuk mengidentifikasi risiko proyek dapat digunakan keamanan jaringan bisnis online. Daftar periksa risiko, metode Delphi, metode curah pendapat, metode diagram alir, work breakdown structure (WBS) risk breakdown structure (RBS), metode analisis skenario, dll. adalah metode identifikasi risiko proyek yang umum digunakan.

5.2 Penilaian Risiko Keamanan Jaringan E-commerce



Gambar 5.4 Penilaian Risiko Keamanan Jaringan E-commerce

Penilaian risiko keamanan jaringan e-commerce adalah proses mengevaluasi jaringan e-commerce dan komponen keamanannya, seperti kerahasiaan, integritas, dan ketersediaan, sesuai dengan standar teknis keamanan jaringan. Tujuannya adalah untuk mendapatkan pemahaman menyeluruh tentang status keamanan jaringan e-commerce, memberikan rekomendasi untuk tindakan pencegahan dan solusi melalui analisis dan evaluasi ilmiah, dan meningkatkan pengawasan dan manajemen keamanan, sehingga menjamin bahwa pengoperasian jaringan e-commerce.

5.2.1 Elemen Penilaian Risiko Keamanan Jaringan Ecommerce

Penilaian risiko keamanan jaringan e-commerce mencakup elemen seperti misi, aset, nilai, ancaman, kerentanan, peristiwa, risiko, risiko residual, persyaratan keamanan, dan langkah-langkah keamanan. Misi adalah pekerjaan yang dilakukan oleh perusahaan e-niaga melalui sistem jaringan. Perusahaan platform telah muncul sebagai akibat dari perkembangan ekonomi platform Internet, yang telah menjadi pelaku dan penyelenggara pasar. Beberapa bahkan telah berkembang menjadi infrastruktur yang memiliki fitur produk kuasi-publik dan bergantung pada jaringan untuk mencapai misinya, menunjukkan betapa pentingnya penilaian risiko.

Selain itu, komponen lain dari penilaian risiko keamanan situs web e-commerce, seperti aset, nilai aset, ancaman, kerentanan, peristiwa, risiko, risiko residu, persyaratan keamanan, tindakan keamanan, dan elemen lainnya, berbeda dari penilaian risiko keamanan informasi. Penilaian risiko keamanan jaringan e-commerce berfokus pada sistem cyber, aset cyber, nilai cyber, dan informasi cyber e-commerce.

5.2.2 Proses Penilaian Risiko Keamanan Jaringan E-commerce



Gambar 5.5 Memahami Penilaian Risiko Keamanan Jaringan E-commerce

Analisis risiko, penilaian risiko, keputusan keamanan, dan pemantauan keamanan adalah beberapa aspek yang termasuk dalam penilaian risiko jaringan e-commerce.

Seperti yang ditunjukkan pada **Gambar 5.5**, keempat sesi ini terdiri dari proses dinamis yang dikenal sebagai penilaian risiko keamanan jaringan e-commerce. Sesi pertama adalah analisis risiko keamanan jaringan e-commerce, yang bertujuan untuk memperkirakan kemungkinan ancaman jaringan e-commerce dan kerugian yang dapat disebabkan oleh kerentanan sistem. Kerentanan dan ancaman adalah dua objek utama untuk menentukan risiko, karena ancaman dan kerentanan sama dengan risiko, dan risiko adalah hasil dari kombinasi

ancaman dan kerentanan. Serangan yang mungkin terjadi pada proses manajemen atau jaringan komputer dikenal sebagai kerentanan.

Ancaman keamanan jaringan e-commerce adalah sumber peristiwa yang dapat membahayakan objek perlindungan keamanan jaringan e-commerce, yang biasanya mencakup target serangan, subjek serangan, dan perilaku serangan. Perlindungan tingkat keamanan 2.0 dengan jelas menekankan pentingnya kesadaran situasional dan merekomendasikan kemampuan untuk menganalisis jenis serangan baru untuk mengidentifikasi, mengkhawatirkan, dan menganalisis berbagai jenis peristiwa keamanan. Misalnya, Persyaratan Dasar Perlindungan Tingkat Keamanan Jaringan Teknologi Keamanan Informasi (GB / T 22239- 2019) menetapkan bahwa langkah-langkah teknis harus dilakukan untuk menganalisis perilaku jaringan dan melakukan analisis serangan jaringan, terutama jenis serangan jaringan baru. Sebelum melakukan analisis risiko, aset jaringan biasanya juga perlu diidentifikasi dan dievaluasi.

Dalam sesi kedua, risiko keamanan jaringan e-commerce dievaluasi. Ada dua metode untuk menilai risiko keamanan jaringan e-commerce: evaluasi risiko kuantitatif dan evaluasi risiko kualitatif. Evaluasi risiko kuantitatif biasanya menggunakan fungsi distribusi probabilitas, dengan distribusi probabilitas risiko yang paling umum adalah distribusi normal. Metode evaluasi risiko kuantitatif yang umum meliputi analisis faktor, analisis klaster, model deret waktu, analisis regresi, dan sebagainya evaluasi risiko kualitatif adalah proses evaluasi dampak dan kemungkinan risiko yang teridentifikasi yang digunakan untuk menentukan dampak potensial dari risiko terhadap keamanan jaringan. Sebagai contoh, evaluasi peristiwa serangan jaringan dapat dilakukan dalam empat aspek: kesulitan deteksi, kesulitan serangan, frekuensi serangan, dan dampak. Kesulitan deteksi mengacu pada kesulitan untuk mendeteksi dan menemukan serangan jaringan, sedangkan kesulitan serangan mengacu pada seberapa mudah target serangan jaringan dapat dicapai. Frekuensi serangan juga merupakan frekuensi serangan itu sendiri.

Dampak adalah hasil dari serangan jaringan. Keempat komponen ini biasanya dinilai dengan skala lima poin. Skor tertentu diberikan sebelum menghitung nilai penilaian risiko keseluruhan. Untuk mengetahui nilai total penilaian risiko, gunakan rumus berikut.

Nilai penilaian risiko keseluruhan = Kesulitan deteksi
+ Kesulitan serangan × 2
+ Frekuensi serangan 3×
+ Dampak × 4

Tabel 5.1 Nilai risiko keseluruhan dan tingkat risiko

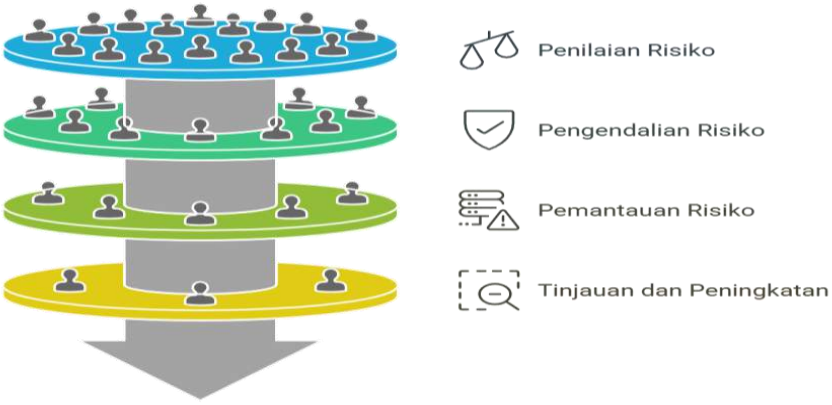
Nilai penilaian risiko secara keseluruhan	Tingkat risiko
<10	Sangat rendah
10-35	Rendah
35-40	Tinggi
>40	Sangat tinggi

Nilai risiko secara keseluruhan, yang ditunjukkan pada **Tabel 5.1**, digunakan sebagai dasar untuk menentukan tingkat risiko. Pemindaian kerentanan juga dapat digunakan untuk menilai risiko keamanan jaringan e-bisnis karena dapat menemukan kelemahan dan kelemahan sistem serta menunjukkan kemungkinan serangan.

Keputusan risiko keamanan jaringan e-commerce dibuat di sesi ketiga. Keputusan ini didasarkan pada hasil evaluasi risiko yang dilakukan untuk menentukan berbagai strategi pengendalian risiko, seperti penghindaran risiko, pengalihan risiko, pengurangan risiko, penerimaan risiko, dan sebagainya. Lihat konten terkait di 4.3.1. Anda dapat menerima risiko saat tingkat risiko rendah; namun, saat tingkat risiko tinggi, Anda harus segera mengambil tindakan perlindungan dan memperbaiki kerentanan untuk mengurangi risiko.

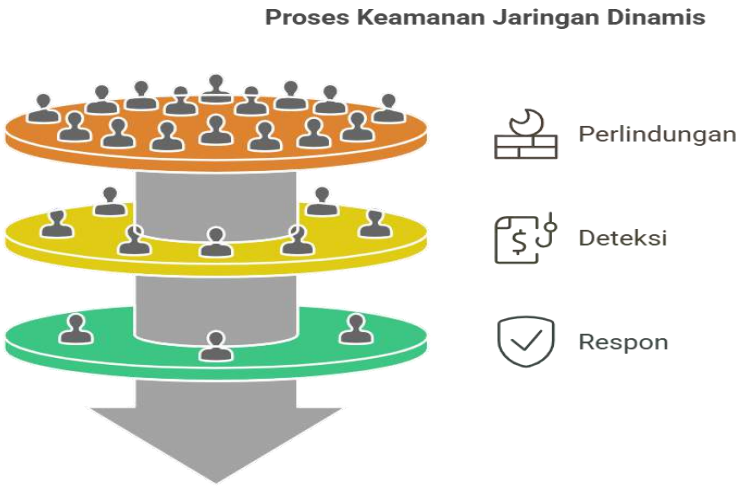
Bagian 4 membahas pengawasan ancaman keamanan jaringan e-commerce. Selama operasi e-commerce, jaringan akan berubah karena perubahan perangkat keras dan perangkat lunak jaringan, peningkatan, dan lainnya. Perubahan ini mengubah status aset jaringan asli, membuat penilaian risiko sebelumnya tidak relevan. Pemantauan keamanan memiliki kemampuan untuk melacak berbagai aset dalam sistem jaringan e-commerce secara real time dan mencatat dan menemukan perubahan dalam operasi. Ini memungkinkan mereka untuk menilai secara akurat status operasional jaringan e-commerce.

5.3 Implementasi Pengendalian Risiko Keamanan Jaringan Ecommerce

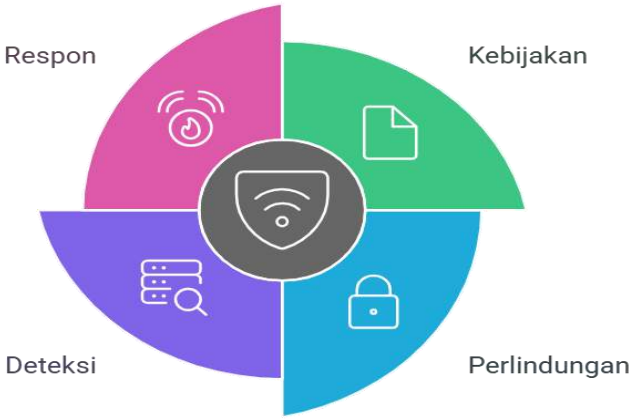


Gambar 5.6 Mengelola Risiko Keamanan Jaringan Ecommerce

5.3.1 Model Keamanan Jaringan



Gambar 5.7 Model PPDR



Gambar 5.8 Model PDRR

keamanan jaringan memberikan penjelasan singkat tentang proses yang terlibat dalam keamanan jaringan, dinamik yang dapat digunakan untuk mengarahkan penyebaran dan pengelolaan tugas keamanan jaringan.

Di bidang keamanan jaringan, ada beberapa model keamanan jaringan, dan model PPDR dan PDRR adalah yang paling umum digunakan. Model PPDR merupakan prototipe dari model keamanan dinamis, yang terutama terdiri dari empat bagian: aturan, perlindungan, deteksi, dan tanggapan, seperti yang ditunjukkan pada **Gambar 5.7** dan **Gambar 5.8**. Perlindungan, deteksi, dan tanggapan adalah sistem keamanan jaringan yang lengkap dan dinamis, dan model PDRR dianggap sebagai model keamanan jaringan yang lengkap. Perlindungan adalah sistem yang dikenal untuk semua masalah keamanan (kerentanan) melalui adopsi langkah-langkah yang efektif, seperti enkripsi data, tanda tangan digital, otentikasi,

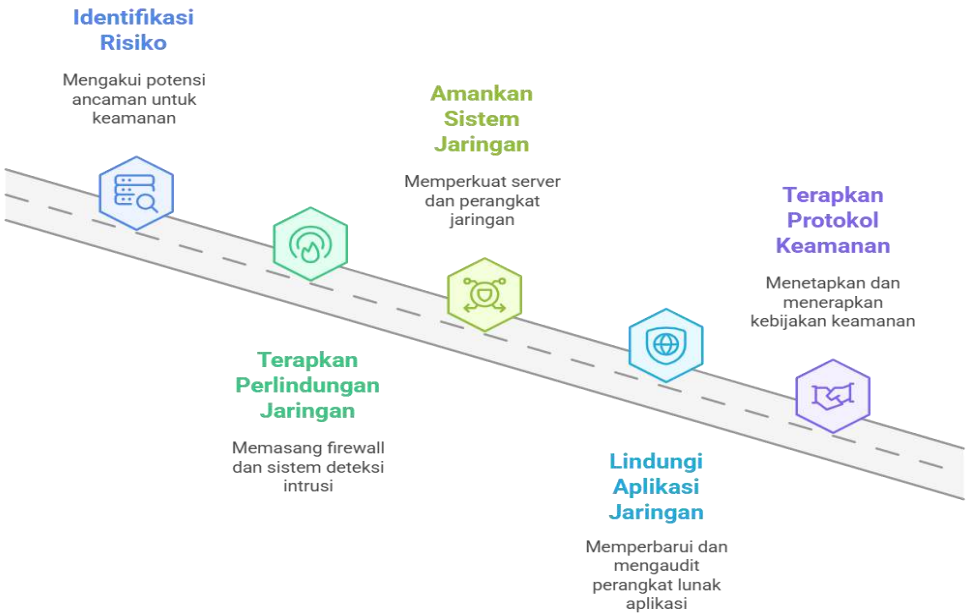
pemindaian kerentanan, kontrol akses, firewall, perangkat lunak antivirus, dan penambalan untuk menghentikan serangan yang mungkin terjadi.

Peristiwa yang muncul setelah pemrosesan disebut respons. Peristiwa lain terutama termasuk tanggap darurat dan peristiwa lain yang harus ditangani. Respon juga mencakup konsultasi, pelatihan, dan bantuan teknis. Pemulihan adalah peristiwa keamanan di mana sistem kembali ke keadaan semula atau lebih aman dari keadaan semula. Memperbaiki atau mengembalikan sistem, mengambil data yang hilang, dan pekerjaan lainnya termasuk dalam kategori ini.

Konsep waktu didefinisikan kembali oleh model PDRR, yang menyatakan bahwa deteksi dan respons yang tepat waktu adalah keamanan dan deteksi dan pemulihan yang tepat waktu adalah keamanan.

Namun, kedua model tersebut berfokus pada teknologi daripada manajemen. Pengendalian risiko keamanan jaringan e-commerce adalah tindakan yang dinamis, menyeluruh, dan menantang yang membutuhkan kombinasi elemen manajemen dan teknis untuk melindungi jaringan e-commerce dengan lebih baik. Metode pengendalian risiko keamanan jaringan dari sudut pandang teknis dan manajemen akan dibahas berikut ini.

5.3.2 Tindakan Teknis



Gambar 5.9 Langkah-langkah Keamanan untuk E-commerce

Langkah-langkah teknis yang diambil untuk mengendalikan risiko keamanan jaringan e-commerce termasuk perlindungan keamanan jaringan, perlindungan keamanan sistem jaringan, dan perlindungan keamanan sistem jaringan, keamanan aplikasi jaringan, protokol keamanan e-commerce, dan sebagainya.

1. Perlindungan keamanan jaringan

Kontrol akses, teknologi firewall, sistem deteksi intrusi, virus komputer dan teknologi perlindungan, jaringan pribadi virtual, dan teknologi keamanan jaringan yang sedang berkembang adalah beberapa contoh perlindungan keamanan jaringan.

(1) Kontrol akses

Masalah legitimasi pengunjung diselesaikan oleh kontrol akses autentikasi, tetapi masalahnya adalah bagaimana pengunjung dengan identitas yang sah dapat mengakses sumber daya sistem. Kontrol akses adalah prosedur atau kebijakan manajemen perangkat keras, perangkat lunak, dan organisasi yang mengesahkan atau membatasi akses berdasarkan keabsahan identitas. Ini memantau dan merekam upaya akses pengguna dan menentukan apakah akses diizinkan. Kontrol akses dapat mencakup mengelola akses pengguna, menentukan tanggung jawab pengguna, mengontrol akses jaringan, sistem operasi, dan aplikasi, serta komputasi mobile dan pekerjaan dari jarak jauh, tergantung pada kebutuhan bisnis.

Kontrol akses mencakup komponen seperti subjek, objek, kebijakan, izin, dan otorisasi. Subjek dari kontrol akses adalah entitas yang melakukan aktivitas dan yang melakukan operasi akses. Subjek adalah objek yang dapat diakses oleh pengguna, seperti file, database, proses, program, komputer, printer, media penyimpanan, dll. Subjek dapat berupa apa pun yang digunakan oleh pengguna, seperti terminal komputer, terminal genggam, atau file. Kebijakan kontrol akses adalah seperangkat aturan yang membatasi akses subjek ke objek tersebut, dan aturan-aturan ini menentukan cara subjek dapat mengakses objek tersebut, sehingga memastikan bahwa penggunaan objek Ketika seseorang memiliki akses ke objek, izin mengacu pada cara mereka dapat melakukan apa pun padanya, seperti membaca, menulis, mengubah, menyalin, menghapus, menjalankan, dll. Metode yang digunakan untuk mengatur hak akses subjek disebut otorisasi. Ada banyak cara untuk mengontrol akses. Ini termasuk kontrol akses preventif, kontrol akses korektif, kontrol akses administratif, kontrol akses logis dan teknis, dan kontrol akses fisik, antara lain. Setiap metode memiliki peran yang berbeda. Kontrol akses preventif menghentikan operasi yang tidak perlu atau tidak sah. Kontrol akses korektif mengembalikan sistem ke keadaan normal setelah operasi yang tidak perlu atau tidak sah selesai.

Kontrol akses administratif adalah penerapan dan pengendalian kontrol akses di seluruh dunia berdasarkan kebijakan keamanan dan prosedur penegakan organisasi. Mekanisme perangkat keras atau perangkat lunak yang dikenal sebagai kontrol akses logis atau teknis digunakan untuk mengontrol akses ke sumber daya dan sistem. Kontrol akses fisik adalah

penghalang fisik yang mencegah orang langsung mengakses sistem. Prinsip-prinsip tertentu digunakan saat membuat kebijakan kontrol akses. Prinsip-prinsip ini termasuk prinsip hak istimewa terkecil, prinsip kebocoran terkecil, dan prinsip pemisahan tugas. Prinsip hak istimewa terkecil mengacu pada hak yang diberikan kepada setiap subjek (pengguna atau proses) dalam jaringan untuk melakukan operasi tertentu. Prinsip kebocoran terkecil mengacu pada hak yang diberikan kepada subjek sesuai dengan prinsip meminimalkan jumlah informasi yang perlu diketahui oleh pengguna atau proses. Prinsip hak istimewa terkecil Kontrol Akses Diskresioner (DAC), Kontrol Akses Wajib (MAC), dan Kontrol Akses Berbasis Peran (RBAC) adalah beberapa kebijakan kontrol akses yang umum.

Kontrol akses otonom memungkinkan subjek untuk membuat pembatasan khusus pada kontrol akses, yang berarti pemilik sumber daya sistem dapat bebas menentukan hak akses orang lain ke sumber daya. Kontrol akses paksa melarang subjek untuk melakukan apa pun. Dalam kebijakan kontrol akses ini, subjek dan objek biasanya diberi nilai dan tag, dan hak akses ditentukan sesuai dengan nilai dan tag tersebut. Pemilik sumber daya tidak memiliki hak untuk memberikan sumber daya mereka kepada subjek lain, dan semua kontrol akses kebijakan ditentukan oleh sistem.

Peran adalah serangkaian tindakan dan tugas yang diperlukan untuk melakukan aktivitas tertentu. Kontrol akses berbasis peran menetapkan peran untuk subjek kontrol akses dan memungkinkan konfigurasi dan perubahan hak kontrol akses pengguna yang fleksibel. Dalam lingkungan jaringan terbuka, konsep "domain" telah ditambahkan ke ketiga kebijakan kontrol akses umum ini. Selain itu, protokol untuk mengontrol akses telah muncul, termasuk akses terkait ruang-waktu, akses berbasis tugas, dan akses terdistribusi. Kebijakan kontrol akses baru berdasarkan kepercayaan, fitur, dan perilaku telah muncul sebagai akibat dari munculnya model komputasi baru seperti komputasi di mana-mana, komputasi seluler, dan komputasi awan. Bagaimana kontrol akses diatur juga menentukan seberapa efektif mereka bekerja. Administrator ditugaskan untuk mengelola akun pengguna, hak akses, dll. melalui manajemen kontrol akses. Manajemen akun pengguna, audit operasional, pelacakan akun, pemantauan sistem, dan manajemen hak akses adalah tugas utama manajemen kontrol akses. Manajemen akun mencakup pembuatan akun pengguna, pengaturan, dan penutupan.

Departemen SDM mengajukan permintaan pembuatan akun untuk karyawan baru, dan administrator keamanan perusahaan dan manajer departemen melakukan verifikasi. Karyawan dididik tentang kebijakan keamanan perusahaan setelah akun dibuat. Hak istimewa akun awal harus diubah ketika posisi karyawan berubah. Akun harus ditutup, dihapus, atau dicabut setelah karyawan mengundurkan diri. Manajemen kontrol akses mencakup audit operasi,

pelacakan akun, dan pemantauan sistem. Ini melacak dan memantau tindakan subjek selama proses pembuatan akun pengguna, verifikasi, dan otorisasi.

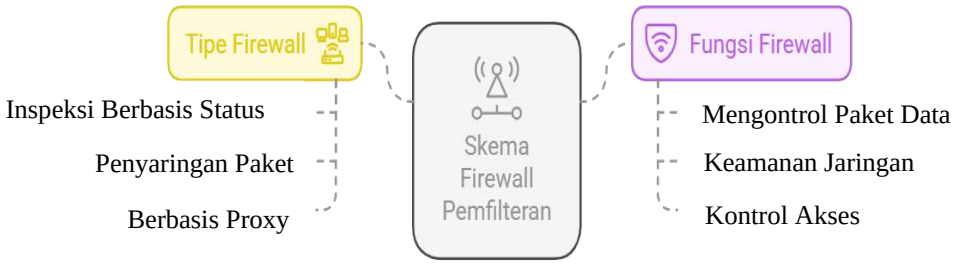
Untuk menentukan subjek mana yang memiliki akses ke objek mana, prinsip hak istimewa terkecil harus digunakan. Tiga tag subjek biasanya digunakan: pengguna, pemilik, dan administrator. Orang yang memiliki akses ke objek sistem, melakukan operasi tertentu, atau menyelesaikan tugas tertentu disebut pengguna. Mengklasifikasikan dan menandai barang adalah tanggung jawab pemilik. Administrator biasanya pengguna akhir sistem, pemilik biasanya CEO, ketua, atau kepala departemen, dan administrator biasanya orang teknis atau administrator keamanan sistem. Sistem memerlukan penyimpanan dan perlindungan objek yang tepat selama operasi sehari-hari. Selain itu, pedoman pemisahan tugas dan tanggung jawab digunakan untuk mengelola hak akses dan izin. Ini memastikan bahwa seseorang tidak dapat menghindari atau menonaktifkan mekanisme keamanan.

(2) Teknologi firewall

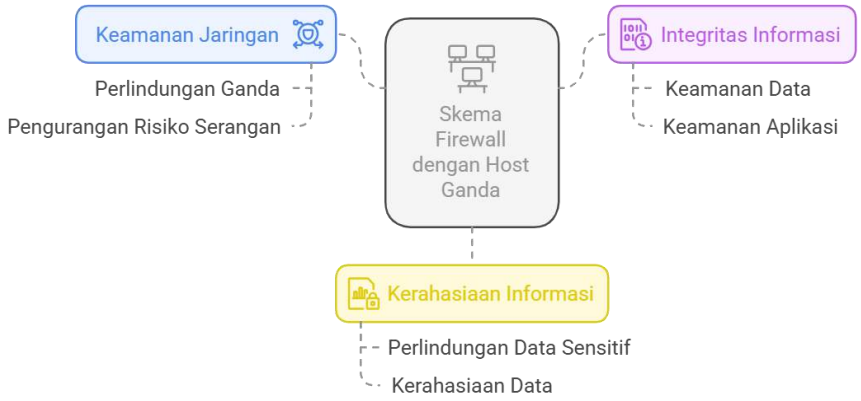
Banyak orang menggunakan teknologi firewall untuk melindungi jaringan mereka. Firewall adalah alat yang paling efektif untuk mencegah penyusupan ilegal ke intranet perusahaan saat terhubung ke Internet. Firewall adalah sistem atau kelompok sistem yang mengatur akses antara dua jaringan. Firewall menyaring layanan yang tidak aman dan pengguna ilegal, memantau dan mengaudit akses jaringan, memperkuat kebijakan keamanan jaringan, dan mengintegrasikan mekanisme untuk memantau aktivitas apa pun antara intranet perusahaan dan Internet. Ini secara logis dapat memisahkan dua jaringan dengan tingkat keamanan yang berbeda, membatasi akses ilegal atau kebocoran informasi, dan pada saat yang sama menganalisis data yang melewati firewall. Firewall juga dapat melakukan banyak tugas lain. Ini termasuk penerjemahan alamat jaringan, jaringan pribadi virtual, otentikasi, kontrol broadband, analisis pengembaraan, dan audit log, antara lain. Meskipun demikian, firewall memiliki kelemahan dan keterbatasan. Misalnya, firewall tidak dapat mencegah serangan yang tidak melewati firewall; tidak dapat mencegah serangan jahat dari orang dalam; tidak dapat menghentikan pengiriman program atau file yang terinfeksi virus; dan firewall hanya dapat berfungsi sebagai pencegahan pasif dan tidak dapat menahan serangan baru. Firewall dapat diklasifikasikan menjadi firewall pemfilteran grup, firewall server proxy, firewall deteksi status, dan firewall adaptif berdasarkan prinsip teknisnya. Firewall dapat dibagi menjadi firewall FTP, firewall login jarak jauh, firewall email, firewall virus, dan firewall khusus lainnya berdasarkan lingkungan perangkat keras mereka.

Firewall terbagi menjadi dua kategori: firewall perangkat lunak dan perangkat keras, menurut cara mereka digunakan. Firewall perangkat lunak digunakan sebagai perangkat lunak

murni dan berjalan pada host yang dipilih. Firewall perangkat lunak biasanya berfungsi sebagai pintu gerbang intranet perusahaan, seperti SkyNet Firewall, 360 Security Guard, dll. Mereka mencapai teknologi penyaringan firewall berkecepatan tinggi dan mengisolasi jaringan internal dan eksternal melalui kombinasi perangkat lunak dan perangkat keras. Firewall pemfilteran grup, firewall host host ganda, firewall host terlindung, firewall subnet terlindung, dan lainnya adalah beberapa arsitektur firewall yang umum digunakan.



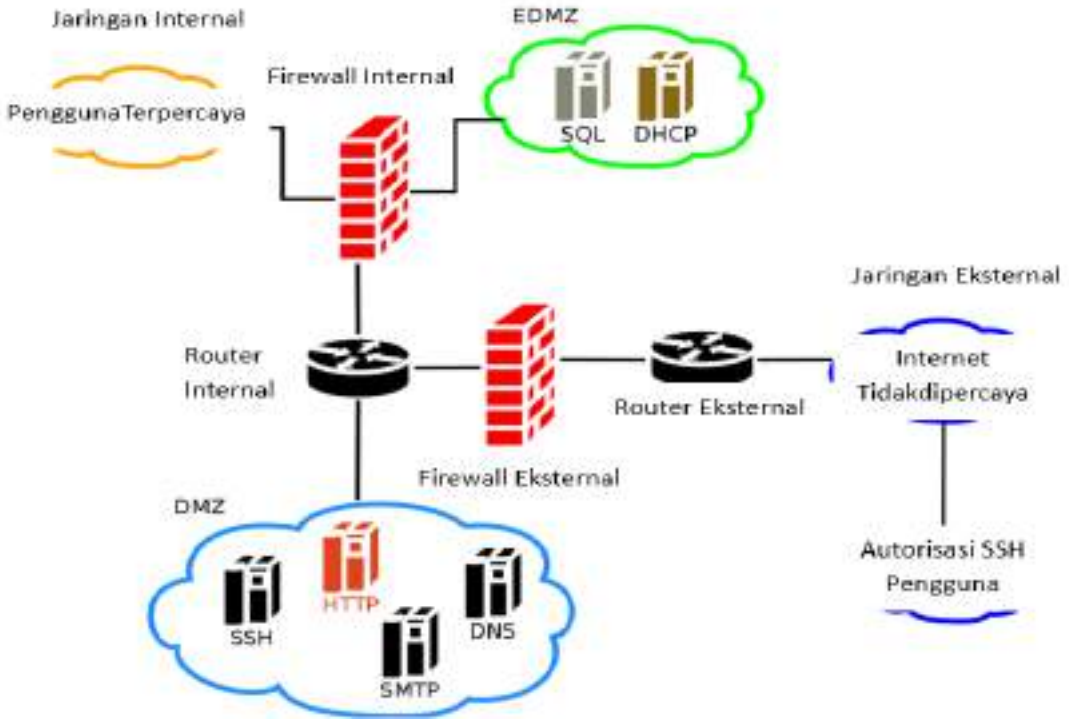
Gambar 5.10 Skema Firewall Pemfilteran: Tipe dan Fungsi



Gambar 5.11 Skema Firewall dengan Host Ganda



Gambar 5.12 Skema firewall host yang memblokir



Gambar 5.13 Diagram skematik firewall subnet terlindung

Pada **Gambar 5.10**, router pemfilteran paket ditunjukkan dan dikonfigurasi untuk melakukan fungsi pemfilteran paket. Router pemfilteran kelompok biasanya menggunakan kebijakan keamanan ekstrim "mengizinkan segala sesuatu kecuali yang dilarang", tetapi perlindungan keamanannya tidak efektif. Ketika jaringan rusak, penyerang hampir tidak dapat dilacak dan serangan jaringan bahkan sulit dideteksi. **Gambar 5.11,** menunjukkan skema firewall host dual-homed. Firewall dual-homed host adalah komputer yang dikonfigurasi dengan dua kartu jaringan dan memiliki dua port jaringan berbeda; satu port menghubungkan intranet perusahaan ke jaringan eksternal, dan yang lainnya menghubungkan intranet perusahaan ke jaringan eksternal. Perangkat lunak server proxy digunakan pada host dual-homed host untuk memisahkan intranet perusahaan dari jaringan eksternal, sehingga pengguna intranet perusahaan hanya dapat mengakses sumber daya yang ada di jaringan eksternal melalui proxy. Setelah penyerang merusak host intranet perusahaan dan membuatnya dapat dirutekan, firewall dilewati, dan setiap orang di jaringan eksternal dapat mengakses intranet perusahaan sesuka hati mereka.

Seperti yang ditunjukkan pada **Gambar 5.12**, firewall host benteng biasanya memiliki dua penghalang: satu adalah bastion host, yang merupakan satu-satunya host yang dapat diakses oleh intranet perusahaan dan jaringan eksternal, dan yang lainnya adalah router penyaringan paket, yang bertanggung jawab untuk menghubungkan ke jaringan. Karena dua hambatan tersebut, orang luar tidak dapat secara langsung mengakses intranet perusahaan. Jika

dibandingkan dengan firewall pemfilteran paket atau firewall host dual-homed, jenis firewall ini lebih praktis dan aman. Subnet terlindung, atau zona demiliterisasi (DMZ), dipisahkan dari intranet perusahaan dan jaringan eksternal dengan firewall subnet terlindung, yang digunakan dua router, seperti yang ditunjukkan pada **Gambar 5.13**. Arsitektur perutean terlindung digunakan oleh firewall ini, yang dikonfigurasi dengan tiga NIC dan menghubungkan ke tiga jaringan berbeda: jaringan eksternal, subnet terlindung, dan intranet perusahaan.

Host benteng adalah satu-satunya host yang dapat diakses melalui intranet perusahaan dan jaringan eksternal. Namun, aturan pemfilteran rute terlindung memeriksanya. Dua router terlindung dan host benteng merupakan tiga penghalang firewall ini. Firewall subnet terlindung memiliki keamanan yang lebih tinggi dan lebih cocok untuk melindungi jaringan besar, tetapi juga lebih mahal karena ketiga penghalang tersebut cukup sulit bagi penyerang untuk melewatinya.

(3) Sistem Deteksi Intrusi

Untuk keamanan jaringan, sistem deteksi intrusi (IDS) melacak intrusi, merekam bukti, melacak intrusi, memulihkan atau memutuskan jaringan, dan tindakan perlindungan lainnya. Ini berfungsi sebagai garis pertahanan tambahan setelah firewall dan memiliki kemampuan untuk menutupi kekurangan firewall. Generator peristiwa, penganalisis peristiwa, basis data peristiwa, dan modul respons adalah komponen sistem deteksi intrusi. Deteksi intrusi mencakup aktivitas ilegal oleh pengguna internal yang sah yang telah melampaui hak istimewa mereka, serta serangan atau probe berbahaya dari luar. Sistem akan secara aktif mengambil tindakan untuk mencegah serangan setelah terdeteksi. Metode utama sistem deteksi intrusi adalah mengumpulkan data di beberapa titik penting dalam sistem atau jaringan dan menganalisisnya untuk menemukan pelanggaran kebijakan keamanan dan tanda-tanda serangan.

Dalam kebanyakan kasus, deteksi intrusi terdiri dari tiga langkah: pengumpulan data, analisis data, dan respons. Pengumpulan data berfokus pada data jaringan, sistem, dan pengguna. Ini dapat diperoleh dari lalu lintas jaringan, informasi log sistem, paket jaringan, perilaku eksekusi program yang tidak biasa, perubahan pada direktori dan file sistem, dan informasi alarm dari sistem pendeteksi penyusupan lainnya. Generator peristiwa mengumpulkan dan mengubah data menjadi peristiwa, yang kemudian didistribusikan ke seluruh sistem. Analisis data adalah bagian penting dari deteksi intrusi; peran utamanya adalah melakukan analisis data mendalam dan menghasilkan peristiwa berdasarkan hasilnya, lalu meneruskan peristiwa tersebut ke modul respons. Berbagai teknik yang biasa digunakan untuk melakukan analisis data termasuk pencocokan pola, analisis statistik, dan analisis integritas.

Basis data peristiwa terdiri dari berbagai data perantara dan data akhir, dan penganalisis peristiwa dapat d Setelah mendeteksi intrusi, sistem deteksi intrusi akan merespons tepat waktu. Ada dua jenis respons: respons aktif yang dapat secara efektif mengontrol penyusup dan ruang lingkupnya. Respons pasif hanya melihat intrusi dan mengeluarkan peringatan, tetapi tidak mengambil tindakan pengendalian. Firewall dan firewall lain dapat bekerja sama dengan sistem deteksi intrusi untuk merespons serangan jaringan dan meningkatkan kemampuan manajemen keamanan sistem. Deteksi anomali, deteksi analisis tanda tangan, dan metode inspeksi mode campuran adalah teknik deteksi intrusi yang paling umum digunakan. Deteksi intrusi anomali juga disebut sebagai deteksi intrusi berbasis perilaku. Perilaku intrusi berbeda dari perilaku normal subjek, menurut sistem deteksi intrusi. Selama proses memantau perilaku pengguna melalui program pemantauan, peristiwa intrusi diidentifikasi dan alarm dikeluarkan. Penyusupan adalah perilaku yang tidak sesuai dengan rutinitas.

Metode untuk mendeteksi intrusi anomali termasuk analisis statis, imunisasi komputer, metode jaringan syaraf tiruan, metode reorganisasi data, dan analisis perilaku. Teknik deteksi intrusi ini memiliki keuntungan seperti kemampuan untuk mendeteksi aktivitas pengguna internal yang melangkah terlalu jauh dan portabilitas yang lebih baik. Namun, mereka memiliki kekurangan, seperti tingkat alarm palsu yang tinggi, waktu deteksi yang lama, dan efisiensi deteksi yang rendah. Deteksi analisis fitur, juga dikenal sebagai deteksi penyalahgunaan atau deteksi penyalahgunaan, adalah untuk menganalisis intrusi yang diketahui dan kerentanan sistem, mempelajari karakteristik intrusi dan kerentanan sistem, membuat deskripsi deterministik dari serangan atau metode intrusi yang diketahui, dan merepresentasikannya dalam pola untuk membentuk perpustakaan fitur intrusi. Ketika peristiwa yang diaudit cocok dengan pola dalam perpustakaan fitur, itu dianggap prinsip analisis fitur sederhana, akurasi peramalan dan pendeteksiannya tinggi, tetapi intrusi dan kerentanan sistem yang tidak dimasukkan ke dalam pustaka fitur tidak dapat diidentifikasi dan diperingatkan, dan cenderung melewatkan laporan, serta portabilitas sistem yang buruk. Untuk memanfaatkan keduanya, teknik deteksi pendekatan gabungan menggunakan deteksi intrusi anomali dan analisis fitur. Pendekatan hibrida memungkinkan sistem deteksi intrusi mendeteksi serangan berdasarkan atribut serangan yang diketahui dan pola yang belum dikonfirmasi, seperti jumlah percobaan login oleh pengguna tertentu. Sistem deteksi intrusi berbasis host, sistem deteksi intrusi berbasis jaringan, sistem deteksi intrusi federasi, dan sistem deteksi intrusi terdistribusi adalah beberapa jenis sistem deteksi intrusi yang paling umum digunakan. HIDS berbasis host mengidentifikasi penyusupan dengan melihat dan menganalisis catatan audit dan file log komputer host. File log mencatat semua aktivitas sistem host, seperti panggilan sistem, hasil

program, dan kapan dan di mana pengguna masuk. Namun, sistem deteksi intrusi berbasis host tidak cocok untuk deteksi intrusi waktu nyata karena merupakan teknologi analisis dan pelacakan "setelah fakta" yang hanya dapat mendeteksi peristiwa intrusi yang telah terjadi.

IDS berbasis jaringan (NIDS) menggunakan paket jaringan mentah sebagai sumber data untuk analisis serangan, dan adaptor jaringan memantau dan menganalisis semua data yang dikirim melalui jaringan secara real time. Setelah serangan terdeteksi, modul responsnya mengirimkan pemberitahuan, alarm, dan koneksi titik akhir untuk menanggapi serangan tersebut. Sistem deteksi intrusi ini memiliki beberapa keuntungan, termasuk deteksi dan respons dalam waktu nyata; kemandirian yang lebih besar, karena tidak bergantung pada platform sistem yang dipantau; target yang tidak dapat dideteksi dengan mudah; dan kemampuan untuk mendeteksi upaya serangan yang gagal.

Sistem deteksi bersama adalah kombinasi firewall dan sistem deteksi intrusi yang memanfaatkan kedua teknologi keamanan untuk mencegah intrusi. Sistem deteksi bersama dan sistem deteksi intrusi biasanya digunakan di dalam firewall; namun, sistem deteksi intrusi juga dapat ditempatkan di dalam firewall atau di luar firewall, sesuai dengan jenis sistem deteksi intrusi yang digunakan, atau di lokasi utama lainnya.

Sistem Deteksi Intrusi Terdistribusi (DIDS) biasanya menggunakan deteksi terdistribusi, pendekatan manajemen terpusat, untuk menganalisis log audit dan aliran data jaringan dari sistem host; firewall akan menambahkan aturan untuk mencegah serangan ulang setelah menerima informasi serangan kembali dari sistem deteksi intrusi, meningkatkan kemampuan keamanan dan perlindungan jaringan.

(4) Virus komputer dan teknologi perlindungan

komputer telah muncul satu demi satu sebagai akibat dari kemajuan teknologi jaringan komputer, yang sangat mengancam keamanan jaringan komputer. Sejumlah besar virus diciptakan dan disebarluaskan dengan cepat, menyebabkan kerugian besar bagi pengguna jaringan komputer. Sebagaimana dinyatakan dalam Peraturan Republik Rakyat Tiongkok tentang Perlindungan Keamanan Sistem Informasi Komputer, virus komputer adalah sekumpulan instruksi atau kode program yang dimasukkan ke dalam program komputer untuk mengganggu fungsi komputer atau merusak data, mempengaruhi penggunaan komputer, dan menggandakan diri. Dalam kebanyakan kasus, virus komputer bersifat programatik, menular, tersembunyi, laten, dapat diaktifkan, dan memiliki target. Selama media yang dapat bertukar data, seperti media penyimpanan mobile dan berbagai jaringan, virus komputer dapat menyebar. Saluran transmisi jaringan termasuk email, mengunduh file, menjelajahi halaman web, pengirim pesan instan, terminal ponsel, situs web phishing, dll. Media penyimpanan

seluler termasuk CD-ROM, DVD, hard disk seluler, disk U, kartu CF, kartu SD, Memory Stick, dll. Jenis dan jumlah virus komputer meningkat setiap tahun sebagai akibat dari perkembangan dan meluasnya penggunaan teknologi komputer. Virus-virus ini juga meningkatkan tingkat dan cakupan kerusakannya. Akibatnya, teknologi antivirus komputer berkembang juga.

Karena masalah utama dalam perlindungan virus komputer adalah "menemukan" virus, deteksi virus yang akurat merupakan komponen penting dari teknologi perlindungan virus. Saat ini, teknologi deteksi yang digunakan untuk mencegah virus komputer terutama terdiri dari teknologi deteksi tradisional berdasarkan kode fitur, teknologi deteksi dinamis berdasarkan perilaku, teknologi deteksi berbasis cloud, dan teknologi deteksi cerdas berdasarkan data besar dan kecerdasan buatan.

Selain itu, tujuan pemindaian kerentanan sebagai teknologi perlindungan virus komputer adalah untuk mencegah masalah sebelum terjadi, sehingga jaringan terlindung dari serangan virus yang disebabkan oleh kerentanan.

Teknologi pemindaian kerentanan dapat dibagi menjadi dua kategori berdasarkan jenis targetnya. Kategori pertama adalah pemindaian sistem, yang mencakup sistem, aplikasi, atau perangkat yang telah digunakan dalam skala besar. Jenis target ini mencakup sistem operasi desktop atau seluler, seperti Windows, Mac, Apple iOS, Android, perangkat jaringan, protokol/port, aplikasi layanan, dll. Kategori kedua adalah pemindaian sistem, yang mencakup sistem operasi sistem operasi desktop atau seluler. Untuk memulai, pemindaian aplikasi menggunakan protokol kontrol eksternal untuk membuat skenario cacat, menyesuaikan vulnerabilitas, dan mengatur parameter input aplikasi sesuai dengan persyaratan skenario. Kemudian, pemindaian membandingkan hasil yang dikembalikan dengan hasil yang diharapkan dari cacat. Akhirnya, kerentanan ditentukan oleh pemindaian ini. Perlindungan virus komputer dapat mencakup pencegahan teknis dan normatif. Salah satu contoh tindakan pencegahan teknis yang dapat diambil termasuk:

Pertama, gunakan semua fitur pemantauan perangkat lunak antivirus dan selalu instal dan perbarui. Perangkat lunak antivirus yang paling populer termasuk 360 Security Guard, Rising Star, Kingsoft Antivirus, dan Kaspersky, antara lain. Gunakan fungsi pemantauan waktu nyata untuk memastikan pembaruan basis data virus perangkat lunak antivirus secara tepat waktu, dan lakukan deteksi virus dan pembersihan sistem secara teratur.

Kedua, segera memperbaiki kerentanan keamanan sistem dan perangkat lunak aplikasi adalah metode pencegahan virus yang efektif untuk memutakhirkan sistem operasi dan menambalnya, karena virus terutama menyerang kerentanan sistem operasi. Banyak aplikasi

perangkat lunak juga memiliki kerentanan yang dapat dengan mudah diserang oleh virus, sehingga perlu ditambal.

Ketiga, aktifkan firewall jaringan di dalam jaringan. Dengan mengatur kebijakan kontrol akses yang tepat, firewall ini dapat menyaring data yang ditransmisikan dalam jaringan dan secara efektif mencegah serangan dari jaringan eksternal.

Keempat, sesuaikan tingkat keamanan peramban.Untuk mengurangi risiko kode dan kontrol berbahaya seperti ActiveX, jangan sembarangan menurunkan tingkat keamanan.

Kelima, sebelum menggunakan media penyimpanan yang dapat dilepas untuk pertukaran data, periksa USB flash drive atau CD-ROM untuk virus. Jangan membuka USB flash drive atau CD yang tidak diketahui asalnya sesuka hati.

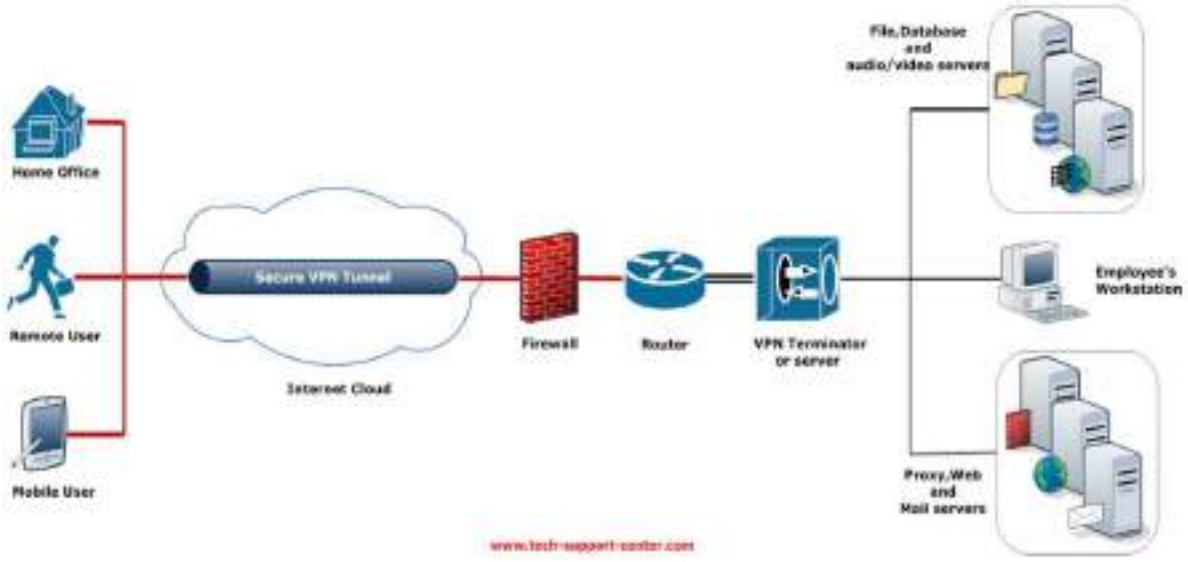
Keenam, administrator jaringan dapat menonaktifkan beberapa port TCP yang digunakan oleh virus Trojan pada switch atau firewall. Ini akan mencegah virus Trojan berjalan dan menyebar.

Ketujuh, lakukan penggunaan teknologi antivirus perangkat keras. Contohnya, meskipun kartu antivirus memiliki kemampuan yang lebih terbatas, mereka akan lebih efektif dalam mencegah virus dan worm yang menggunakan kerentanan buffer overflow untuk menyerang. Metode normatif berikut dapat digunakan.

Pertama, tingkatkan kesadaran keamanan Anda dengan membangun kebiasaan pengoperasian komputer yang baik, membuat cadangan file data sistem secara teratur, menghilangkan virus saat menggunakan perangkat penyimpanan eksternal, dan menghindari mengunduh dan mendistribusikan file yang tidak diketahui asalnya. Kedua, pastikan untuk menggunakan versi awal perangkat lunak jaringan. Ketiga, jangan pergi ke situs web yang ilegal atau tidak dikenal. Jika Anda ingin mengunduh perangkat lunak, cobalah untuk melakukannya dari situs web yang legal dan profesional. Keempat, gunakan perangkat lunak antivirus untuk mengidentifikasi lampiran email yang berisi file atau dokumen yang dapat dieksekusi. Jika demikian, berhati-hatilah sebelum membukanya. Kelima, lakukan cadangan sistem dan data yang berkualitas tinggi. GHOST membantu mencadangkan sistem, yang dapat mempercepat pemulihan sistem setelah rusak. Jangan lupa untuk menjaga keamanan dokumen dan data penting. Keenam, jika sistem memiliki virus, perangkat lunak antivirus harus menggunakan fungsinya untuk memeriksa dan membunuh virus. Namun, jika perangkat lunak antivirus terpaksa ditutup oleh virus, Anda harus menggunakan metode profesional untuk menghapus virus secara manual, atau menginstal ulang sistem operasi terlebih dahulu, lalu menggunakan perangkat lunak antivirus untuk menghapus virus. Ketujuh, sesuaikan kata sandi login sistem dan fungsi layanan jaringan. Gunakan kata sandi keamanan tinggi yang terdiri dari

kombinasi huruf, angka, dan simbol bahasa Inggris. Kata sandi harus panjangnya lebih dari delapan digit. Cobalah menghentikan layanan jaringan yang tidak perlu juga.

(5) Jaringan Pribadi Virtual



Gambar 5.14 Diagram jaringan pribadi virtual

Seiring perkembangan ekonomi global, semakin banyak perusahaan yang membuka cabang dan menjalankan operasinya di berbagai lokasi. Untuk mencapai tujuan pengiriman informasi, karyawan dari berbagai lokasi di organisasi pengelompokan perlu berkoneksi satu sama lain. Perusahaan sering menyewa jaringan data digital (DDN) jalur khusus atau jalur jarak jauh, tetapi ini mahal. Dengan menggunakan virtual private network (VPN), orang dari luar dapat dengan aman mengakses jaringan privat internal dari jarak jauh melalui jaringan publik. Ini adalah metode yang murah dan aman untuk meningkatkan intranet.

Sebuah istilah "jaringan pribadi virtual" mengacu pada penggunaan teknologi keamanan informasi untuk menghubungkan intranet bisnis yang tersebar di seluruh Internet, atau untuk menghubungkan satu atau lebih pengguna jarak jauh ke jaringan area lokal. Jaringan pribadi virtual adalah saluran transmisi khusus virtual yang dibuat di Internet. Selama komunikasi, mereka hanya menggunakan sebagian bandwidth jaringan dan melepaskan sebagian bandwidth ini setelah komunikasi berakhir.

Seperti yang ditunjukkan pada **Gambar 5.14**, jaringan virtual privat terdiri dari tiga kategori: jaringan virtual akses jarak jauh (Access VPN), jaringan virtual intra-perusahaan (Intranet VPN), dan jaringan virtual perusahaan yang diperluas (Extranet VPN). Pengguna yang berada di jarak jauh dapat melakukan panggilan ke penyedia layanan Internet (ISP) lokal dengan menggunakan saluran VPN virtual di jaringan publik. Metode ini dikenal sebagai Jaringan Pribadi Virtual Akses Jarak Jauh (RAVPN). Metode ini dapat digunakan oleh

karyawan internal untuk pekerjaan mobile dan telecommuting, serta perusahaan untuk memberikan akses aman ke Jaringan Pribadi Virtual Perusahaan Internal (IEVPN) dalam mode bisnis ke konsumen.

Jaringan pribadi virtual perusahaan internal berarti membangun jaringan pribadi virtual pada intranet dengan biaya untuk menghubungkan LAN cabang perusahaan yang terletak di tempat lain dengan LAN kantor pusat perusahaan. Ini memungkinkan perusahaan untuk berbagi sumber daya dan mengirim file di dalam perusahaan. Jaringan Jangkauan Pribadi Virtual Perusahaan (EOVPN). Enterprise outreach VPN berfungsi untuk menghubungkan intranet perusahaan dan mitra melalui teknologi VPN. Ini mirip dengan IEVPN, tetapi karena melibatkan komunikasi antara jaringan perusahaan yang berbeda, lebih banyak perhatian harus diberikan pada koneksi peralatan, koordinasi alamat, perundingan kebijakan keamanan, dll.

Administrator jaringan perusahaan juga harus membuat daftar kontrol akses (ACL) khusus untuk mengidentifikasi hak akses yang sesuai dengan identitas pengunjung, alamat jaringan, dan parameter lainnya. ACL ini memungkinkan pengguna ekstranet untuk mengakses beberapa sumber daya, tetapi tidak semua.

(6) Sistem Deteksi Intrusi

Internet seluler adalah hasil dari penggabungan teknologi komunikasi seluler dan teknologi Internet yang mendalam. Banyak layanan aplikasi baru dan cepat telah muncul untuk mobilitas internet seluler. Namun, keamanan Internet seluler menghadapi tantangan keamanan yang besar karena keterbukaan, heterogenitas jaringan, kemampuan pengorganisasian mandiri, dan fitur lainnya. Ditambah dengan meningkatnya jumlah virus dan perilaku berbahaya berbasis Internet untuk terminal seluler, keamanan Internet seluler menghadapi tantangan keamanan yang besar. Pertama, keamanan terminal seluler. Serangan fisik dari perangkat keras, seperti chip baseband dan perangkat fisik, serangan berbahaya, seperti virus, kode berbahaya, dan situs web phishing untuk sistem operasi, dan ancaman keamanan, seperti penanaman virus, otentikasi identitas, dan akses tidak sah ke perangkat lunak aplikasi, adalah semua bahaya yang menghalangi terminal seluler. Saat ini, metode perlindungan utama yang digunakan adalah adopsi teknologi komputasi yang dapat diandalkan untuk menghasilkan perangkat terminal pintar yang aman dan dapat diandalkan. Teknologi kriptografi enkripsi data yang dikirim dan disimpan di perangkat seluler. Menggunakan teknologi antivirus untuk meningkatkan kemampuan intersepsi dan pemblokiran virus, spyware, dan perangkat lunak abu-abu. Yang kedua adalah keamanan jaringan Internet seluler.

Keamanan jaringan Internet seluler terutama mencakup keamanan perangkat dan lingkungan, keamanan transmisi, dan keamanan informasi. Strategi perlindungan keamanan

yang dapat diadopsi terutama mencakup meningkatkan kemampuan anti-serangan dan anti-intrusi dari peralatan jaringan, sistem terkait, dan basis data; mempertahankan standar terkait jaringan Internet seluler dan meningkatkan pemeliharaan perangkat Internet seluler; Selanjutnya, keamanan aplikasi Internet seluler. Aplikasi Internet seluler termasuk layanan yang ditransfer dari Internet tradisional, aplikasi yang terhubung ke jaringan komunikasi bergerak, dan jenis layanan baru yang dibuat dari kombinasi keduanya.

Aplikasi berbasis Internet seluler sangat kompleks, tetapi otentikasi dapat dilakukan dengan menggunakan teknologi kanalisasi yang aman; kontrol hak akses berdasarkan sertifikat atribut; dan konten web yang tidak diinginkan, spam, dan SMS berbahaya dapat disaring dengan menggunakan teknologi pemfilteran konten seperti teknologi pemfilteran daftar, kata kunci, dan gawang. Yang keempat adalah peraturan yang berkaitan dengan keamanan jaringan Internet seluler. Peraturan dan undang-undang terkait Internet seluler harus ditingkatkan, standar harus ditingkatkan, dan kerja sama dan pertukaran dengan organisasi standardisasi internasional harus diperkuat. Internet of Things (IoT) adalah jaringan yang menggunakan Internet, jaringan telekomunikasi konvensional, dan pembawa informasi lainnya untuk memungkinkan semua objek fisik biasa yang dapat dihubungkan untuk berinteraksi satu sama lain secara independen. IoT terdiri dari semua perangkat yang terhubung ke Internet, yang dapat berkomunikasi satu sama lain dan berbagi data. IoT memiliki banyak aplikasi di banyak bidang, seperti logistik pintar, jaringan pintar, transportasi pintar, pengujian lingkungan, dan aplikasi pengguna terintegrasi seperti aplikasi Web, game online, e-commerce, rumah pintar, dan video on demand.

Akibatnya, teknologi keamanan yang disesuaikan dengan mereka sangat dibutuhkan. Untuk lapisan pengenalan penginderaan, teknik enkripsi yang efektif dan mekanisme manajemen kunci dapat digunakan untuk memastikan kerahasiaan dan otentikasi komunikasi dalam jaringan penginderaan. Untuk lapisan konstruksi jaringan, otentikasi lintas domain dan lintas jaringan, enkripsi ujung ke ujung, algoritme kriptografi yang mendukung multicast dan siaran, dan protokol keamanan dapat digunakan untuk mencapai otentikasi simpul, kerahasiaan, dan integritas data dan aliran data.

Untuk lapisan layanan manajemen, keamanan dapat dicapai dengan menyediakan layanan kerahasiaan dan integritas data berkekuatan tinggi, kontrol akses sumber daya, deteksi intrusi, analisis perintah berbahaya, perlindungan virus, pencadangan dan pemulihan file, mekanisme pemulihan bencana, pemantauan dan pelacakan log, dan identifikasi perangkat seluler, lokasi, dan mekanisme pelacakan. Untuk lapisan aplikasi terintegrasi, perlindungan keamanan dapat dicapai dengan menggunakan kontrol akses aplikasi, mekanisme penyaringan konten,

teknologi perlindungan informasi privasi, teknologi perlindungan kekayaan intelektual perangkat lunak, audit keamanan (seperti mekanisme pelacakan, teknologi forensik komputer), dll.

2. Perlindungan keamanan sistem jaringan

(1) Perlindungan keamanan sistem operasi

Di sini, perlindungan keamanan sistem operasi mengacu pada kontrol perangkat keras dan perangkat lunak sistem komputer oleh sistem operasi dengan fungsi jaringan, yang dapat memberikan perlindungan keamanan yang sesuai untuk yang mengelola sumber daya, seperti perlindungan penyimpanan, perlindungan operasi, identifikasi, dan otentikasi, audit keamanan, dll. Tujuan keamanan ini dapat dicapai melalui sejumlah elemen berikut. Pertama dan terpenting, mekanisme keamanan sistem operasi.

Salah satu contoh mekanisme keamanan sistem operasi adalah kontrol isolasi, kontrol akses, kontrol aliran informasi, dan mekanisme audit. Isolasi adalah teknik umum untuk menghindari bahaya yang disebabkan oleh gangguan timbal balik antara berbagai bagian sistem. Ada empat cara umum untuk mengontrol isolasi: isolasi fisik, isolasi temporal, isolasi logis, dan kriptografi. Isolasi fisik adalah isolasi pada tingkat perangkat fisik atau komponen, sehingga program pengguna yang berbeda menggunakan objek fisik yang berbeda. Isolasi temporal adalah menetapkan periode runtime yang berbeda untuk program pengguna yang memiliki kebutuhan keamanan yang berbeda. Isolasi logis terjadi ketika sistem operasi membatasi area di mana beberapa proses pengguna dapat berjalan dan mencegah proses lain untuk mengakses area yang tidak diizinkan. Kriptografi terjadi ketika sebuah proses menyembunyikan data dan komputasinya sehingga proses lain tidak dapat melihatnya (misalnya, dengan menggunakan metode enkripsi). Jenis isolasi yang disebutkan di atas semakin kompleks dan tidak aman.

Salah satu masalah utama yang harus diselesaikan oleh kontrol akses adalah untuk mengontrol akses ilegal ke sumber daya sistem komputer dan memastikan bahwa subjek hanya dapat mengakses sumber daya dengan otorisasi eksplisit. Kontrol akses dapat dilakukan dengan berbagai cara, seperti kontrol akses otonom, kontrol akses wajib, akses berbasis peran, kontrol akses diskrit (juga dikenal sebagai kontrol akses terkait nama), dan sebagainya. Semua metode ini harus dilaksanakan sesuai dengan prinsip hak minimum dan pembagian maksimum. Prinsip hak minimum mengatakan bahwa setiap subjek memiliki hak istimewa setiap saat hanya dalam batas-batas perlindungan minimum yang terdiri dari hak istimewa yang diperlukan untuk menyelesaikan tugasnya. Sebagai contoh, hak istimewa seorang pengguna super dibagi menjadi hak istimewa yang lebih kecil dan diberikan kepada masing-masing

administrator sistem, sehingga masing-masing administrator sistem hanya memiliki hak istimewa yang lebih kecil daripada hak istimewa pengguna super.

Prinsip pembagian maksimum mengatakan bahwa informasi yang tersimpan dalam sistem (seperti basis data, file disk, dll.) harus tersedia sebanyak mungkin dalam batas-batas tertentu untuk jumlah informasi yang mungkin digunakan. Dalam sistem terbuka, akses ke objek harus diizinkan kecuali secara eksplisit dilarang. Sebaliknya, dalam sistem tertutup, akses hanya diperbolehkan jika secara eksplisit diizinkan. Selain melindungi hak istimewa yang paling sedikit, sistem pertama lebih aman. Yang terakhir sesuai dengan prinsip pembagian maksimum dan lebih murah. Kontrol aliran informasi berarti menentukan hubungan antara kelas keamanan informasi dan kelas keamanan objek yang dapat disimpan, serta hubungan aliran informasi antara objek yang termasuk dalam kelas keamanan yang berbeda. Misalnya, informasi dibagi menjadi tingkat keamanan yang berbeda, seperti sangat rahasia, rahasia, rahasia, dan tidak dikategorikan menurut sensitivitasnya, dan informasi dari setiap tingkat keamanan membentuk kelas keamanan. Saluran tepercaya dan rahasia adalah dua jenis saluran aman untuk aliran informasi. Saluran tepercaya digunakan oleh sistem komputer untuk berkomunikasi dengan sistem operasi melalui aplikasi yang tidak tepercaya. Saluran rahasia diberikan oleh sistem operasi untuk menjamin bahwa aliran informasi tidak dicegat oleh Trojan. Saluran rahasia dapat digunakan oleh proses yang melanggar peraturan keamanan sistem untuk mengirimkan informasi secara ilegal.

Penemuan dan pengendalian saluran rahasia biasanya sulit. Audit adalah proses penelusuran setelah fakta untuk sistem operasi yang aman, yaitu dengan merekam, memeriksa, dan mengaudit tindakan keamanan. Tujuan utamanya adalah untuk menemukan dan mencegah pengguna ilegal merusak sistem dan menunjukkan penyalahgunaan pengguna yang sah. Mekanisme audit harus mengawasi semua operasi sensitif pengguna. Untuk memudahkan analisis dan pelacakan serangan, sistem audit harus mencatat serangan atau kejadian sensitif terhadap keamanan. Proses audit biasanya merupakan proses yang terpisah dari fungsi-fungsi lain sistem operasi. Sistem operasi harus menghasilkan, menjaga, dan melindungi proses audit, terutama data audit, dengan membatasi akses pengguna yang tidak berwenang.

Kedua, manajemen hirarki keamanan sistem operasi. Manajemen hirarki keamanan sistem operasi biasanya mempertimbangkan keamanan sistem operasi pada tingkat sistem, tingkat pengguna, dan tingkat file. Tugas manajemen keamanan tingkat sistem adalah mencegah pengguna yang tidak diizinkan untuk masuk ke sistem, sehingga orang lain tidak dapat menggunakan sumber daya sistem secara ilegal. Secara khusus, manajemen keamanan tingkat sistem dapat digunakan melalui registrasi dan login. Ini mengacu pada pemberian hak akses

kepada pengguna untuk mengakses file dan menentukan ukuran file yang dapat dilakukan pengguna berdasarkan klasifikasi pengguna, persyaratan pengguna, dan atribut file. Hak akses juga menentukan operasi apa yang dapat dilakukan pengguna pada file, seperti membuat, menghapus, membuka, membaca, menulis, menanyakan, dan memo.

Identitas dan autentikasi pengguna diperlukan untuk mendapatkan kontrol akses pengguna. Sistem Identifikasi memberikan nama pengguna (pengenal pengguna). Autentikasi adalah proses yang mengidentifikasi seseorang sebagai pengguna. Ini adalah lapisan keamanan di luar sistem. Manajemen keamanan tingkat file berarti mengatur bagaimana pengguna dapat mengakses file melalui administrator sistem atau atribut file.

Menjalankan, menyiratkan, memodifikasi, mengindeks, hanya-baca, menulis, berbagi, dan lain-lain adalah atribut file. Ketiga, jenis sistem pendeteksian dan operasi. Karena sebagian besar kerentanan keamanan berkaitan dengan sistem operasi tertentu, mendapatkan akses ke jenis sistem operasi dan versi host jarak jauh yang tepat sangat penting untuk studi kerentanan keamanan jaringan komputer. Deteksi jenis sistem operasi host target dapat membantu manajemen jaringan dan menentukan kerentanan host target. Jenis sistem operasi dapat diidentifikasi dengan dua metode utama: deteksi aktif dan deteksi pasif. Teknologi deteksi aktif secara aktif dan sengaja mengirim paket probe ke sistem target, menentukan jenis sistem operasi host target dengan mengekstrak dan menganalisis informasi karakteristik dari paket respons. Deteksi aktif lebih akurat dan efisien, tetapi mungkin terdeteksi oleh firewall jaringan target atau sistem deteksi penyusupan. Metode ini sangat rahasia dan hampir tidak dapat ditemukan oleh host mana pun di jaringan.

(2) Perlindungan keamanan sistem basis data

Sistem basis data adalah sistem komputer yang melakukan basis data dan pengelolaannya menggunakan teknologi basis data, yang merupakan kumpulan media penyimpanan, objek pemrosesan, dan sistem manajemen. Sistem basis data termasuk basis data, sistem manajemen basis data, platform perangkat keras, sistem operasi yang mendukung sistem manajemen basis data, dan perangkat lunak lainnya. Administrator basis data, analis dan perancang basis data, pengguna, dan media Basis data adalah pusat transaksi dan sistem pembayaran elektronik dalam e-commerce, di mana data pribadi mitra bisnis dan pelanggan disimpan. Perlindungan sistem basis data terutama mencakup persyaratan keamanan sistem basis data, kerangka kerja keamanan sistem basis data, keamanan basis data dan keamanan jaringan, serta pencadangan dan pemulihan basis data. Pertama, kebutuhan keamanan sistem basis data serupa dengan kebutuhan keamanan sistem komputer lainnya, seperti sistem operasi. Dalam hal keamanan

sistem basis data, ada lima elemen penting: integritas, kerahasiaan, pengendalian, ketersediaan, dan privasi.

Database memiliki berbagai tingkat integritas, termasuk integritas elemen data (untuk menjaga keakuratan konten elemen data, seperti bidang data dan item data), integritas fisik (untuk memastikan bahwa data tidak terpengaruh oleh kegagalan fisik), dan integritas logis (untuk menjaga struktur dan pemrosesan logis database). Data yang dirahasiakan mencegah orang yang tidak berwenang mengaksesnya. Kemampuan untuk memantau operasi data dan kejadian sistem basis data serta memantau, mencatat, dan melacak kejadian yang mengancam kerahasiaan, integritas, dan ketersediaan dikenal sebagai pengendalian.

Privasi mengacu pada penggunaan sistem basis data dan data untuk melindungi privasi pribadi subjek dari pengungkapan dan penyalahgunaan; ini termasuk kerahasiaan dan integritas, penerimaan akses, dan keakuratan otentikasi. Ketersediaan juga mengacu pada kemampuan untuk memastikan efisiensi operasional sistem dan kenyamanan interaksi manusia-komputer ketika pengguna yang berwenang melakukan operasi normal pada database.

Kedua, kerangka kerja keamanan sistem basis data. Ini mencakup keamanan jaringan, keamanan sistem manajemen basis data, dan keamanan sistem operasi host. Enkripsi data basis data dapat dilakukan pada tiga tingkat keamanan sistem manajemen basis data: sistem operasi, kernel sistem manajemen basis data (DBMS), dan lapisan luar DBMS. Pada tingkat sistem operasi, sistem enkripsi dapat digunakan untuk melakukan operasi enkripsi pada file database, tetapi tidak dapat menghasilkan kunci yang masuk akal. Pada tingkat kernel DBMS, enkripsi menunjukkan bahwa pemrosesan enkripsi dan dekripsi data basis data telah selesai sebelum orang fisik dapat mengakses data. Penggunaan sistem enkripsi basis data sebagai alat lapisan luar DBMS, yang secara otomatis dapat menyelesaikan pemrosesan enkripsi dan dekripsi data basis data sesuai dengan kebutuhan enkripsi, adalah keuntungan, tetapi memiliki beban berat pada server.

Ketiga, keamanan basis data dan perlindungan basis data jaringan. Keamanan basis data mencakup keamanan sistem dan keamanan data, yang mengatur akses dan penggunaan basis data di tingkat sistem dan objek (termasuk penggun) dan keamanan basis data mengatur akses dan penggunaan basis data di tingkat objek (termasuk penggun). Ketika disimpan, database juga dapat dienkripsi. Selain itu, enkripsi di dalam perpustakaan dan enkripsi di luar perpustakaan adalah dua jenis enkripsi basis data yang berbeda. Enkripsi basis data biasanya menggunakan algoritma enkripsi kelompok karena pertimbangan kecepatan enkripsi dan dekripsi. Sebagian besar, sistem manajemen kunci multi-level dan terpusat digunakan untuk mengelola basis data. Keamanan basis data jaringan terdiri dari dua tingkat. Yang pertama

adalah keamanan lapisan periferal, yang mencakup keamanan sistem manajemen basis data, keamanan jaringan yang mentransmisikan data, keamanan sistem operasi, dan layanan aplikasi Web. Yang kedua adalah keamanan lapisan inti, yang mencakup keamanan basis data itu sendiri. Ini mencakup enkripsi basis data, kontrol hierarki basis data, desain sistem pemulihan bencana basis data, dll. Untuk memastikan keamanan database jaringan dan penggunaan teknologi keamanan jaringan pada saat yang sama, kebijakan keamanan tertentu harus diterapkan karena ada faktor keamanan dalam lingkungan operasi dan manajemen operasi database jaringan.

Kebijakan keamanan fisik, keamanan jaringan, dan keamanan manajemen adalah beberapa contoh kebijakan keamanan di sini. Mengelola pengguna basis data jaringan juga mencakup mengotentikasi pengguna, mengelola akses ke sumber daya, dan memantau audit dari sisi klien dan server. Keempat, penyimpanan dan pemulihan database. Jika sistem database gagal, database dapat rusak dan data dalam database dapat hilang sebagian atau seluruhnya. Beberapa alasan utama kegagalan database termasuk kegagalan peralatan atau sistem, kegagalan jaringan, kegagalan daya, kesalahan program, ketidakmampuan untuk beroperasi, serangan hacker, bencana alam, dll. Kegagalan database dapat mempengaruhi ketersediaan database, sehingga sangat penting untuk Pemindahan sebagian atau seluruh data basis data ke media penyimpanan lain disebut pencadangan basis data. Ini dilakukan untuk mencegah data hilang karena masalah sistem atau kesalahan operasi yang tidak terduga. Pencadangan basis data harus mempertimbangkan hal-hal berikut. Pertama adalah konten pencadangan dan periode pencadangan. Konten pencadangan database dan periode pencadangan harus mencakup semua data, tabel (struktur), pengguna, objek, dan log perubahan, serta item lainnya. Tingkat kegagalan, rasio operasi baca/tulis, dan tingkat kegagalan biasanya menentukan periode pencadangan. Untuk database umum, dapat dicadangkan seminggu sekali; log transaksi harus dicadangkan setiap hari atau setiap beberapa jam.

Selanjutnya, teknologi pencadangan. Pencadangan data dan pemeliharaan log adalah dua metode pencadangan yang umum. Pencadangan statis dan dinamis berbeda dalam statusnya. Pencadangan statis dilakukan ketika tidak ada transaksi yang sedang berjalan dalam sistem. Pencadangan dinamis adalah jenis pencadangan yang memungkinkan akses atau perubahan pada basis data selama pencadangan; dengan kata lain, pencadangan dan operasi transaksi dapat dilakukan sekaligus. Pencadangan data dapat dibagi menjadi pencadangan bertahap atau pencadangan penuh, bergantung pada metode pencadangan yang digunakan.

Pencadangan penuh mencadangkan seluruh isi database setiap kali; pencadangan bertahap mencadangkan hanya konten yang diperbarui sejak pencadangan terakhir. Pencadangan penuh

dinamis, pencadangan bertahap dinamis, pencadangan penuh statis, dan pencadangan bertahap statis. Log adalah file yang merekam setiap operasi pembaruan database. Ini memungkinkan pemulihan database ketika database gagal.

Pencadangan dapat dilakukan secara berkala dengan menggunakan alat pencadangan yang disediakan oleh sistem manajemen database untuk menyimpan sebagian atau seluruh data, dan dengan menggunakan alat pemeliharaan log untuk menyimpan rekaman audit transaksi dan perubahan database. Setelah database atau data rusak secara tidak sengaja, pemulihan database, juga disebut pemuatan ulang data atau pemasukan kembali, adalah proses menginstal ulang database menggunakan cadangan yang ada.

Metode berikut dapat digunakan untuk pemulihan data. Metode 1: Pemulihan cadangan menggunakan database cadangan untuk pemulihan setelah kegagalan yang tidak disengaja misalnya, kegagalan media adalah kegagalan yang lebih serius yang hanya dapat diperbaiki dengan menggunakan database cadangan. Metode 2: Pemulihan log transaksi: ini biasanya digunakan dalam kasus kegagalan transaksi. Kegagalan transaksi adalah ketika transaksi secara tidak sengaja berakhir sebelum waktunya. Pemulihan log transaksi menggunakan file log transaksi untuk memulihkan transaksi yang belum selesai atau belum selesai, mulai dari nilai transaksi yang belum selesai dalam urutan catatan log transaksi. Ini membatalkan operasi yang telah dilakukan dan mengembalikannya ke kondisi di awal transaksi, yang biasanya dilakukan secara otomatis oleh sistem.

Metode Tiga: Strategi pencerminan teknik mirroring mengacu pada dua database identik yang disimpan pada perangkat yang berbeda pada saat yang sama. Kedua database ini disebut database utama dan database mirror, dan pembaruan dari salah satu dari mereka akan tercermin secara bertahap ke database lainnya. Karena pencerminan database dilakukan dengan mereplikasi data, replikasi data sering mengurangi efisiensi operasi sistem, sehingga dalam aplikasi praktis, biiasanya dipilih untuk mencerminkan data kunci dan file log, daripada mencerminkan seluruh database.

3. Perlindungan keamanan aplikasi web

(1) Perlindungan keamanan web

Banyak bisnis dan lembaga pemerintah memiliki situs web yang dipersonalisasi. Serangan peretas, gangguan virus, spionase komersial, kode berbahaya, penipuan dan pencurian, kesalahan dan kesalahan manajer atau personel terkait, dan kerentanan antarmuka adalah beberapa ancaman yang menghalangi server Web yang mengatur situs Web. Namun, firewall dan sistem deteksi intrusi tidak dapat menghilangkan semua kerentanan server Web. Persyaratan keamanan Web meliputi sistem keamanan Web, sistem keamanan server Web, dan

sistem keamanan browser Web. Pertama, sisi server Web dan sisi klien Web memiliki persyaratan keamanan yang tinggi karena mereka dirancang untuk server Web dan workstation Web (klien). Untuk server Web, keamanan perlu menjaga keamanan layanan Web yang tersedia, memastikan bahwa informasi yang dipublikasikan adalah asli dan akurat, dan untuk workstation Web, keamanan perlu menjaga keamanan layanan Web yang tersedia, meliputi Kedua, sistem keamanan web.

Sistem keamanan web terutama mencakup perangkat lunak klien (seperti browser Web), peralatan komputer yang menjalankan browser dan sistem operasinya (sistem host), klien Web yang terletak di sistem keamanan jaringan area lokal, sistem keamanan Internet, dan server Web yang terletak di sistem keamanan jaringan area lokal, dan komputer yang menjalankan perangkat lunak server dan sistem operasi (sistem host). Dalam hal struktur keamanan server Web, kebijakan keamanan mencakup teknologi dan alat keamanan host dan jaringan, konfigurasi aplikasi Web, mekanisme otentikasi layanan Web, firewall dan log, dll. Tujuan utama kebijakan keamanan untuk penyedia layanan Web adalah untuk mengatur siapa yang dapat mengakses dokumen Web dan menentukan otoritas dan tanggung jawab orang-orang yang memiliki akses ke dokumen Web. Untuk meningkatkan keamanan server Web, Anda harus menyiapkan zona keamanan berikut ini. Zona Infrastruktur: Zona infrastruktur menunjukkan di mana server berada di jaringan. Zona ini harus melindungi server dari teknik penyusupan seperti penyadapan data, pemetaan jaringan, dan pemindaian port. Komponen terpusat melindungi semua server yang menyediakan layanan Internet dan berada di jaringan yang terisolasi yang dikenal sebagai zona demiliterisasi (DMZ).

Melacak server Web yang telah disusupi sangat penting karena server tersebut dapat menjadi basis serangan terhadap server lain. Tempat Protokol Jaringan Pengaturan server Web harus diubah untuk mencegah serangan karena beberapa protokol jaringan mudah digunakan oleh penyerang untuk melakukan serangan atau sabotase. Selain itu, paket IP dengan opsi perutean sumber harus ditolak, ICMP mengalihkan, dan operasi ping untuk menyiarkan alamat. Dengan fungsi penyaringan tambahan yang sesuai, tingkat keamanan dapat ditingkatkan. Zona Layanan: Zona layanan menentukan layanan mana yang diperlukan dan biasanya menerapkan kebijakan keamanan "jika tidak perlu, nonaktifkan semua". Konfigurasikan hanya layanan-layanan pada server Web yang diperlukan untuk melakukan operasi yang diperlukan, jika tidak maka akan memberikan lebih banyak titik serangan bagi penyerang. Zona layanan harus memastikan bahwa layanan memiliki tingkat keamanan yang memadai dan bahwa layanan yang tidak aman diganti dengan yang lebih aman. Setiap layanan harus dikonfigurasi secara

terpisah untuk keamanan. Konfigurasi server yang buruk dapat menyebabkan akses yang tidak sah atau menjadi sasaran serangan.

Perbaiki Area. Instalasi program, terutama program yang sangat istimewa, harus dibatasi pada komponen yang diperlukan untuk operasinya. Selain itu, prosedur keamanan seperti pencadangan rutin dan deteksi penyusupan berbasis host harus dilakukan. Ketiga, langkah-langkah pencegahan berikut dapat diambil oleh manajemen keamanan server Web. Batasi pengguna untuk membuka akun di server Web, secara teratur menghapus akun pengguna yang sudah kedaluwarsa, dan menerapkan persyaratan keamanan yang lebih tinggi pada akun pengguna yang dibuka di server Web. Jalankan berbagai program layanan (seperti ftp, mail, dan layanan Web, dll.) pada berbagai server, dan cobalah untuk mematikan layanan yang tidak diperlukan. Selalu catat aktivitas server Web dan periksa log server untuk mengidentifikasi semua peristiwa yang mencurigakan. Tentukan izin dan fitur file sistem server Web dengan benar. Selain itu, tentukan grup umum untuk dokumen yang dapat diakses. Selanjutnya, tetapkan izin hanya-baca untuk dokumen tersebut. Simpan direktori dokumen Web di tempat yang berbeda dari direktori lain, seperti direktori FTP.

Batasi akses dari alamat IP tertentu dan batasi izin baca dan tulis pada direktori, yang menyimpan program dan skrip yang dapat dieksekusi, untuk mencegah penyerang masuk. Selain melakukan hal-hal di atas, Anda harus segera meng-upgrade atau menambal program dan memberikan perlindungan khusus untuk cadangan, seperti enkripsi. Keempat, sistem keamanan peramban web. Banyak ancaman keamanan menyertai peramban web. Misalnya, penyerang dapat menggunakan fitur panggilan otomatis browser Web untuk mendapatkan akses yang tidak sah ke komputer yang menjadi ancaman. Contoh tambahan adalah file cookie yang memungkinkan server Web untuk menyimpan informasi tentang dokumen Web tertentu ketika pengguna mengaksesnya melalui browser Web. Setelah pengguna mengakses dokumen Web tersebut lagi melalui browser, server secara otomatis mengambil informasi ini untuk digunakan dalam dokumen Web tersebut. Hal ini memungkinkan penyebaran data pribadi seperti nama pengguna, kata sandi, atau nomor kartu kredit, sehingga meningkatkan risiko penyebaran data pribadi. Spoofing web mudah dilakukan karena halaman web mudah direplikasi. Kode berbahaya, kerentanan pada peramban itu sendiri, dan lainnya juga dapat membahayakan peramban Web.

Untuk memastikan keamanan browser Anda, ada banyak cara yang dapat Anda gunakan. Untuk fungsi panggilan otomatis browser, Anda dapat mengikuti langkah-langkah berikut: jangan mengandalkan rekomendasi orang lain dan dengan santai mengubah konfigurasi program eksternal; jangan membiarkan program eksternal berbahaya mengakses situs web; dan

jangan sembarangan menambahkan program eksternal dan memperhatikan program eksternal yang tidak default. Untuk menghindari spoofing web, berikut adalah langkah-langkah yang dapat diambil: mengatur preferensi peramban JavaScript, ActiveX, dan Java; gunakan petunjuk peramban sepenuhnya; perhatikan dengan cermat apakah sertifikat situs sesuai dengan apa yang disebutkan; dan jangan tertipu oleh karakter yang mirip. Selain itu, pemutakhiran dan penambalan yang tepat waktu dapat memperbaiki kerentanan peramban.

(2) Perlindungan keamanan email

Email telah menjadi sarana penting bagi orang-orang untuk berkomunikasi dengan dunia luar. Kerentanan perangkat lunak, situs web phishing, virus, dll., sering menggunakan email untuk merusak, yang mengarah pada kebocoran informasi pribadi pengguna dan bahkan nomor akun, kata sandi, dan informasi lainnya. Kasus-kasus yang berkaitan dengan keamanan email sering terjadi. Misalnya, kerentanan berisiko tinggi Office dapat menyebabkan pencurian informasi privasi pengguna dalam skala besar oleh email berbahaya; dokumen berbahaya menyebar melalui lampiran email spam dengan kata-kata seperti "pesanan" dan "pembelian produk" untuk mengelabui pengguna agar mengklik dan mencuri informasi privasi mereka. Keamanan sistem email secara langsung mempengaruhi keamanan email. Sebuah sistem email mungkin memiliki celah keamanan pada kata sandi, transmisi, sistem perangkat lunak, dan aspek-aspek lainnya. POP3, SMTP, IMAP4, dan protokol email lainnya menggunakan plaintext dalam pengiriman dan pengunduhan, yang juga menjadi kerentanan keamanan pada sistem. Selain itu, virus email, spam, dll., juga merupakan ancaman besar bagi keamanan email, sehingga metode yang berbeda perlu digunakan untuk mengatasi dan mempertahankannya. Pertama, pencegahan kerentanan email.

Email yang berbeda harus menggunakan metode pencegahan yang berbeda, secara khusus ada beberapa metode sebagai berikut. Tingkatkan keamanan kata sandi email. Disarankan untuk menggunakan kombinasi karakter yang tidak beraturan dengan panjang yang cukup sebagai kata sandi; mengatur pertanyaan permintaan kata sandi, dan balasan yang sesuai menjadi rumit; jangan menyimpan kata sandi saat menggunakan komputer umum untuk mengakses Internet untuk mencegah kebocoran kata sandi; beroperasi secara pribadi untuk mengirim dan menerima email, dan mengosongkan semua catatan bisnis di akhir operasi; ketika menggunakan email sendiri di depan umum, pastikan untuk keluar dari sistem email secara normal; membiasakan mengganti kata sandi secara teratur dianjurkan sekali dalam tiga bulan atau lebih untuk kata sandi yang penting; usahakan untuk tidak menggunakan satu kode untuk berbagai tujuan; dan mengatur kata sandi yang berbeda untuk sistem yang berbeda. Enkripsi email.

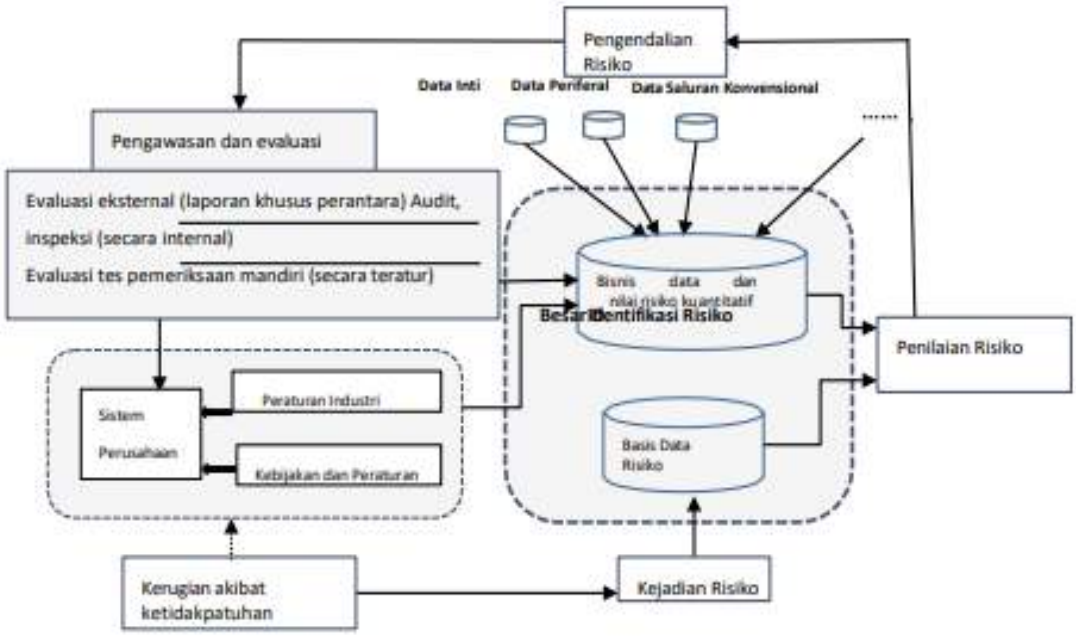
Mengadopsi teknologi email aman end-to-end untuk mengenkripsi email guna memastikan bahwa isi email bersifat rahasia, tidak dapat diubah, dan tidak dapat disangkal dalam proses pengiriman hingga penerimaan. Standar email aman endto-end yang biasa digunakan di Internet adalah standar S/MIME dan sebagainya. Meningkatkan keamanan dan keandalan server email. Serangan pada server email terutama dibagi menjadi dua jenis: intrusi jaringan dan gangguan layanan, dan hasil yang baik dapat dicapai dengan mengambil tindakan yang tepat untuk menangani kedua metode ini. Membatasi penggunaan perangkat lunak klien email. Perangkat lunak klien email adalah lingkungan untuk operasi pengiriman dan penerimaan email. Dan pembatasannya adalah garis pertahanan pertama terhadap kerentanan, yang dapat dicapai dengan bantuan alat keamanan pihak ketiga atau alat enkripsi untuk mencapai pembatasan yang sesuai.

(3) Perlindungan keamanan data besar

Dengan munculnya Internet seluler, Internet of Things, Triple Play, komputasi awan, Web2.0, dan teknologi lainnya dalam beberapa tahun terakhir, berbagai perangkat terminal terus merekam perilaku informasi yang kompleks yang dilakukan oleh manusia. Perilaku ini termasuk pencarian informasi, membaca, komunikasi, belanja, dan tindakan lainnya di Internet dan ruang fisik. Kumpulan data atau kelompok data yang tidak dapat dikumpulkan, disimpan, dikelola, atau dianalisis oleh perangkat lunak basis data tradisional dalam jangka waktu tertentu adalah disebut "big data". Dengan demikian, metode pemrosesan baru hanya dapat digunakan untuk menunjukkan sifat-sifatnya yang sangat berharga, masif, dan beragam sebagai aset informasi.

Nilai, variasi, volume, dan kecepatan adalah empat ciri data besar. Volume adalah istilah yang mengacu pada skala data yang sangat besar, mulai dari terabyte hingga PB atau bahkan lebih tinggi. Data terstruktur, tidak terstruktur, dan semi-terstruktur termasuk dalam kategori kompleksitas dan variasi jenis data yang berbeda. Data terstruktur didefinisikan sebagai data yang memiliki karakteristik tetap dan dapat dimodelkan dengan tabel dua dimensi yang dikenal sebagai model relasional. Ini biasanya disimpan dalam basis data relasional. Data tidak terstruktur adalah data yang tidak dapat dijelaskan dengan mudah dan biasanya diwakili oleh tabel dua dimensi atau bahasa alami. Contoh data tidak terstruktur termasuk teks, dokumen yang diformat, email, mikroblog, geolokasi data, weblog, gambar, video, audio, dan berbagai laporan. Data yang berada di antara data terstruktur dan data tidak terstruktur disebut sebagai data semiterstruktur. Dokumen HTML dan XML adalah contoh data semi-terstruktur yang umum. Ketepatan waktu menunjukkan bahwa data dapat dibuat dan diproses dengan sangat cepat. Data dengan kepadatan rendah tetapi nilai yang tinggi disebut nilai. Big data digunakan

lebih banyak di e-commerce. Big data telah mengubah model pengendalian risiko, terutama dalam hal aspek pengendalian risiko.



Gambar 5.15 Model pengendalian risiko data besar

Seperti yang ditunjukkan pada **Gambar 5. 15**, model pengendalian risiko big data mencakup identifikasi risiko, penilaian risiko, pengendalian risiko, pengawasan dan evaluasi, serta elemen penting lainnya. Pengendalian risiko perusahaan e-commerce dan organisasi lain dapat menggunakan model pengendalian risiko big data. Penilaian risiko kredit, kontrol risiko keuangan Internet, dan pemantauan opini jaringan adalah beberapa contoh penggunaan data besar sebagai alat kontrol risiko baru. Sebagai lokasi penting untuk pembuatan, peredaran, dan penerapan data besar, dunia maya telah menjadi sasaran utama serangan siber. Selain menghasilkan nilai yang signifikan bagi berbagai industri dan bisnis, masalah keamanan yang terkait dengan penyimpanan dan transmisi data besar, alat audit data, dan kepercayaan konten data besar adalah beberapa faktor yang membuat penerapan data besar rentan terhadap risiko keamanan.

Di bawah ini, teknik utama untuk melindungi keamanan dan privasi data besar dibahas. Teknologi enkripsi data besar, kontrol akses, prediksi dan pencegahan ancaman, audit dan audit data besar, penemuan kerentanan keamanan data besar, dan teknologi otentikasi berbasis data besar adalah beberapa teknologi penting untuk perlindungan keamanan data besar. Teknologi yang digunakan untuk enkripsi data besar solusi untuk pemrosesan data teks sandi adalah enkripsi yang dapat dicari dan homomorfik. Untuk melindungi kerahasiaan data, enkripsi

homomorfik dibahas dalam Bab 4 melakukan komputasi pada teks plain, mengenkripsinya setara dengan enkripsi, dan kemudian melakukan komputasi pada teks sandi.

Sifat homomorfis algoritma enkripsi memungkinkan pengguna untuk menghindari kebocoran data ketika mempercayakan data kepada pihak ketiga untuk diproses; ini memecahkan masalah komputasi data besar yang aman. Karena sulit untuk mengindeks data dengan menggunakan teknik enkripsi umum, enkripsi yang dapat dicari dapat memecahkan masalah ketersediaan data yang rendah. Teknik enkripsi yang dapat dicari secara simetris dan asimetris adalah dua jenis utama. Metode untuk Mengontrol Akses teknik kontrol akses terutama digunakan untuk melindungi sumber daya data besar yang dilindungi dari akses yang tidak sah. Untuk mengatasi korelasi spatiotemporal data besar di cloud, beberapa ahli telah mengusulkan kontrol akses berbasis atribut (ABAC, kontrol akses berbasis atribut), kontrol akses berdasarkan enkripsi ulang agen, kontrol akses untuk beberapa pusat otorisasi di lingkungan cloud, dan kontrol akses berbasis lokasi (misalnya, protokol kontrol akses berbasis peran yang sadar lokasi, LARB), antara lain. Namun, pengelolaan hak pengguna menjadi sangat sulit karena terminal pengguna baru, server, penyimpanan, perangkat jaringan, dan sumber daya informasi lainnya terus terhubung ke platform data besar, dan semakin banyak data yang mengalir ke sistem yang berbeda. Selain itu, sangat penting untuk mempelajari pendekatan kontrol akses berbutir halus yang digabungkan; ini termasuk pembagian hak akses berbutir halus dan pembuatan teknik kontrol akses gabungan untuk hak pengguna dan hak data. Teknologi yang digunakan untuk prediksi dan pencegahan ancaman Saat ini, serangan Advanced Persistent Threats (APT) adalah ancaman besar terhadap keamanan data, dan metode utama untuk mencegah serangan APT adalah metode sandbox, deteksi anomali, dan deteksi berbasis memori. Sistem file lokal dan registri, yang merupakan target potensial serangan APT, dipisahkan satu sama lain oleh sistem file virtual, yang merupakan fitur utama metode deteksi sandbox. Sistem file yang sebenarnya tidak akan diubah pada saat yang sama dengan sistem file virtual; sebaliknya, akan dialihkan ke jalur yang berbeda, dan sistem file kemudian disimpan. Di satu sisi, hal ini memungkinkan penyerang untuk menyerang secara bebas di kotak pasir. Di sisi lain, teknik serangan dapat diringkas dengan melihat perubahan yang terjadi pada sistem file, yang memungkinkan penemuan dan penerapan tindakan pencegahan pada sistem file yang sebenarnya.

Namun, metode sandbox kurang fleksibel dan menghabiskan banyak sumber daya. Metode deteksi sandbox mungkin tidak dapat mendeteksi serangan APT di beberapa tempat. Metode deteksi anomali bergantung pada penggunaan jumlah data yang relatif kecil untuk mengidentifikasi anomali dalam lalu lintas jaringan secara keseluruhan, serta untuk mencegah

anomali jaringan tertentu dengan menentukan apakah mereka sesuai dengan model data lalu lintas normal atau bahkan menemukan sumber serangan APT. Metode deteksi berbasis memori menggabungkan metode deteksi keamanan jaringan konvensional dengan metode deteksi lalu lintas penuh. Metode ini membutuhkan pencatatan dan analisis menyeluruh dari banyak log untuk menemukan pola serangan dan bagaimana serangan dapat terjadi. dan memeriksa kemungkinan serangan APT dengan membandingkan informasi umpan balik dari analisis log dan pendekatan deteksi konvensional dengan standar. Metode ini menghadapi masalah utama karena dipengaruhi oleh metode deteksi tradisional yang tidak efisien. Audit keamanan dan metodenya audit keamanan mencakup identifikasi, pencatatan, penyimpanan, dan analisis aktivitas yang terjadi di dalam sistem. Ini mengklarifikasi siapa dan bagaimana data atau layanan dapat diakses, serta memahami dari mana data berasal dan bagaimana digunakan. Ini memungkinkan manajemen data dan deteksi cepat dan penemuan serangan dan perilaku tidak normal lainnya. Untuk audit keamanan, data besar memungkinkan audit dalam berbagai cara. Misalnya, log sistem dapat digunakan untuk melakukan audit keabsahan operasi; perbandingan dapat digunakan untuk melakukan audit integritas informasi pengeluaran aplikasi, dll. Audit teknologi mencakup audit saluran penyimpanan tersembunyi yang menghubungkan berbagai subsistem atau layanan yang termasuk dalam sistem, sehingga mengurangi risiko keamanan sistem. Dengan data besar, auditor pihak ketiga (TPA) dapat digunakan untuk mengaudit. Auditor pihak ketiga bersifat independen dari pelanggan dan platform cloud, sehingga pelanggan dapat mengaudit data yang disimpan dalam cloud. Penemuan Risiko Keamanan Data Besar penemuan kerentanan keamanan big data adalah untuk mengetahui pintu belakang dan masalah keamanan yang ditinggalkan oleh platform big data dan program layanan karena faktor manusia atau kelemahan desain. Ini mencegah penyerang menggunakan kerentanan ini untuk mengakses atau merusak data dan platform big data tanpa izin. Metode seperti pengujian kotak putih, pengujian kotak hitam, pengujian kotak hitam, dan analisis jejak dinamis adalah beberapa metode yang dapat digunakan untuk menganalisis penemuan kerentanan keamanan platform big data. Teknologi otentikasi yang bergantung pada data besar. Teknologi otentikasi berbasis data besar mengacu pada penggunaan teknologi data besar untuk mengumpulkan data tentang perilaku pengguna dan perilaku perangkat. Dengan menganalisis data ini, mereka dapat menentukan identitas dan melakukan otentikasi. Ini dapat menutupi kekurangan teknologi otentikasi tradisional.

Teknologi sistem masuk tunggal, dua faktor, dan multi-faktor adalah beberapa teknologi otentikasi yang umum. Autentikasi identitas dan manajemen identitas di lingkungan komputasi awan yang kompleks diselesaikan dengan teknologi sistem masuk tunggal. Serangan

penolakan layanan, serangan man-in-the-middle, serangan replay, dan serangan dua faktor menolak lainnya teknologi otentikasi multi-faktor meningkatkan keamanan otentikasi dengan menggunakan lebih banyak kredensial keamanan daripada kredensial keamanan konvensional. Teknologi perlindungan privasi data besar yang paling penting termasuk teknologi anonimisasi data besar, teknologi perlindungan privasi diferensial, teknologi penelusuran data, teknologi pengambilan informasi privasi, teknologi penghapusan data tepercaya, dan lainnya.

Teknik yang melindungi privasi dan anonimisasi data besar kontrol atribut dan anonimisasi dapat digunakan untuk memungkinkan rilis dan kueri data anonim tanpa pengetahuan penyerang tentang latar belakang atau sumber data lainnya. Pengaturan atribut pengguna untuk membuat orang lain terlihat atau tidak terlihat dikenal sebagai kontrol atribut. Anonimisasi berarti menyembunyikan atau mengaburkan data seperti nama, nomor ID, alamat, dll., bersama dengan sumbernya saat memberikan data. Untuk mencapai tujuan melindungi privasi pribadi, teknik ini umumnya menggunakan penekanan, generalisasi, pembuatan profil, pengirisan, dan pemisahan untuk memproses data sehingga ada sejumlah individu yang tidak dapat dibedakan dalam data yang dipublikasikan. Dengan demikian, penyerang tidak dapat menemukan orang yang memiliki informasi sensitif. Namun, anonimisasi tidak aman ketika penyerang memiliki latar belakang pengetahuan khusus atau dapat melakukan penautan silang dengan berbagai sumber data. Ini adalah tempat teknik k-anonimisasi diperlukan. Metode ini pertama-tama melakukan praproses pada dataset asli sehingga setiap catatan tidak dapat dibedakan dari setidaknya satu catatan K-1 dalam dataset. Dalam kasus kelompok ekuivalensi, korespondensi satu-ke-satu antara atribut pengenal semu dan atribut privasi tidak ada lagi, melindungi informasi pribadi dari penyusupian. Kumpulan catatan yang memiliki nilai atribut yang sama pada pengenal semu disebut grup ekuivalensi. Dengan kata lain, semua catatan dalam grup ekuivalensi memiliki nilai atribut yang sama pada pengenal semu, sementara nilai atribut lainnya dapat berbeda. Namun, ketika entropi perlindungan privasi dalam kelompok ekuivalensi yang sama kecil, model keragaman-l telah diusulkan. Ini berarti generalisasi lebih lanjut berdasarkan jaminan k-anonimitas sehingga setidaknya l nilai yang berbeda dari atribut sensitif ada dalam setiap catatan kelompok ekuivalensi. Ada metode anonimitas seperti M-invariance, T-closeness, dan HD-composition selain metode di atas. Selain itu, dalam hal penerbitan dan perlindungan data jejaring sosial, karena jejaring sosial berisi banyak informasi sensitif, seperti hubungan tautan, atribut simpul, penanda simpul, dan fitur struktur grafik, dll., anonimitas identifikasi pengguna dan atribut (anonimitas simpul) dan anonimitas hubungan pengguna (anonimitas tepi) dapat digunakan untuk melindungi privasi data jaringan desain.

Metode generalisasi berbasis pengelompokan menggunakan pengelompokan untuk membuat super node dan super edge dalam graf, dan informasi sensitif dari setiap node dan edge dalam graf disembunyikan di super node atau super edge tersebut. Metode ini juga dapat digunakan untuk pengelompokan node, edge, dan node-edge. Metode modifikasi struktur graf berarti mengubah struktur graf dengan menyisipkan dan menghapus node untuk memastikan bahwa node dan edge dapat diidentifikasi ulang. Metode seperti ini biasanya bergantung pada gagasan yang serupa dengan metode k-anonimisasi untuk menghentikan hacker menggunakan struktur jaringan sebagai latar belakang pengetahuan.

Teknik melindungi privasi dengan cara yang berbeda. Teknik perlindungan privasi diferensial adalah metode perlindungan privasi yang baru dan efektif yang didukung oleh teori matematik. Teknik ini mengontrol tingkat perlindungan privasi dan tingkat kehilangan privasi melalui parameter privasi sambil memastikan hasil komputasi tidak terpengaruh oleh penyisipan atau penghapusan catatan dalam kumpulan data tertentu. Selain itu, metode ini tidak peduli dengan latar belakang pengetahuan penyerang, dan privasi arsip tidak terganggu meskipun penyerang memiliki informasi tentang semua arsip kecuali arsip tertentu; ini membuat pendekatan perlindungan privasi yang berbeda sangat terukur. Teknologi perlindungan privasi unik sangat cocok untuk data besar karena skala dan keragamannya. Teknologi untuk mencari data. Menandai sumber data dapat mempersingkat waktu bagi pengguna untuk mengidentifikasi keaslian informasi dan membantu mereka memeriksa kebenaran hasil analisis. Metode penandaan adalah teknik penelusuran data yang paling dasar, yang terutama mencatat metode penghitungan dan asal data. Selain digunakan dalam penelusuran dan pemulihan dokumen, penelusuran data sekarang juga digunakan untuk melindungi privasi data besar. Metode untuk mengumpulkan data privasi untuk kueri yang aman pada basis data outsourcing, teknik pengambilan informasi privasi biasanya digunakan. Ini memungkinkan pengguna meminta data apa pun pada platform layanan yang tidak dapat dipercaya tanpa mengungkapkan informasi sensitif tentang data yang diminta. Meskipun data yang diminta dapat berasal dari sumber publik dan anonim, platform layanan tidak dapat membedakan konten khusus dari data tersebut. Teknik pengambilan informasi privasi terbagi menjadi dua kategori. Yang pertama adalah teknik pengambilan informasi privasi berbasis teori informasi, yang biasanya menyampaikan semua data kepada klien dan memungkinkan pemecah kode lokal; namun, biaya transmisi yang tinggi membuatnya tidak cocok untuk data besar. Kategori kedua adalah teknik pengambilan informasi privasi berbasis perangkat keras, yang biasanya digunakan dalam pencocokan urutan DNA, pengambilan gambar bergambar, dan pencocokan urutan DNA lainnya. Teknik pengambilan informasi privasi mendorong

pengembangan perangkat keras dan perangkat lunak keamanan, tetapi menggunakan teknik ini dalam lingkungan data besar dapat menjadi tantangan. Teknik Penghapusan Data yang Dipercaya setelah menyimpan data di cloud, risiko kebocoran data meningkat karena data mungkin tetap tersimpan secara jahat dan tidak dapat benar-benar dimusnahkan meskipun pengguna mengeluarkan perintah penghapusan. Metode penimpaan biasanya digunakan oleh banyak sistem penyimpanan untuk menghapus data; namun, metode ini bergantung pada karakteristik fisik media penyimpanan fisik. Setelah pemilik data kehilangan kontrol atas media penyimpanan data, metode penimpaan berbasis media penyimpanan menjadi tidak memadai untuk penghapusan data. Penghapusan data tepercaya, juga dikenal sebagai penghancuran aman, adalah ketika orang menghancurkan data secara aman di lokasi dengan menggunakan kunci.

Jika pengguna menggunakan kunci penghancuran aman, data tidak dapat didekripsi dalam waktu polinomial meskipun server yang tidak dapat dipercaya masih menyimpan data teks sandi yang seharusnya dihancurkan oleh pengguna. Ini melindungi keamanan data. Selain itu, ada beberapa pendekatan baru untuk penghapusan data yang dapat diandalkan. Teknik penghapusan data berbasis waktu yang dapat diandalkan, misalnya teknik ini menggunakan sejumlah kecil potongan kunci data yang didistribusikan di berbagai lokasi jaringan dan dihapus setelah waktu yang ditentukan. Penghapusan data tepercaya berbasis kebijakan, yang menggunakan teori graf, kriptosistem simetris, dan teknik berbagi kunci ambang, adalah contoh tambahan.

(4) Perlindungan keamanan komputasi awan

Sumber daya komputasi model komputasi awan meliputi kapasitas komputasi, penyimpanan, dan interaksi, antara lain, dan dapat diskalakan dalam bentuk layanan melalui Internet. Komputasi awan terdiri dari empat kategori berdasarkan cara penyebarannya: awan pribadi, awan publik, awan komunitas, dan awan hibrida. Dalam hal kontrol keamanan, komputasi awan tidak jauh berbeda dari teknologi informasi lainnya. Namun, ada risiko yang berbeda dalam hal model layanan, model operasional, dan teknologi yang digunakan untuk menyediakan layanan terkait. Sebagai contoh, hal ini mengurangi kontrol pengguna terhadap data dan sistem bisnis, meningkatkan kesulitan dalam mendefinisikan tanggung jawab antara pengguna dan penyedia layanan cloud, menimbulkan masalah yurisdiksi yang mungkin, menimbulkan masalah kepemilikan data pelanggan, mengatur perlindungan data yang lebih sulit, meninggalkan sisa data, dan menjadi terlalu tergantung pada penyedia layanan cloud. Pembahasan berikut berkonsentrasi pada teknologi keamanan data komputasi awan, teknologi keamanan aplikasi, otentikasi pengguna yang masif, dan strategi respons keamanan komputasi

awan untuk perusahaan e-commerce. Pertama, teknologi keamanan data komputasi awan: keamanan penyimpanan awan dan transmisi awan. Layanan kelas penyimpanan awan biasanya menggunakan algoritme enkripsi berkualitas tinggi seperti AES, 3DES, dan algoritme enkripsi umum internasional lainnya, atau algoritme enkripsi Cina SM1 (SCB2). Untuk keamanan transmisi awan, teknologi VPN seperti IPSec VPN dan SSL, serta saluran kedua, teknologi keamanan aplikasi.

Teknologi keamanan aplikasi komputasi awan meliputi keamanan terminal pengguna, keamanan aplikasi SaaS, keamanan aplikasi PaaS, dan keamanan infrastruktur IaaS. Keamanan terminal pengguna adalah bagian penting dari keamanan informasi di lingkungan jaringan, dan penggunaan perangkat lunak keamanan yang tepat di terminal pengguna merupakan langkah pertama menuju keamanan cloud. Oleh karena itu, sangat penting untuk memilih penyedia layanan cloud yang dapat menyediakan layanan SaaS. Berikutnya adalah keamanan aplikasi untuk PaaS, yang mengacu pada Platform as a Service, sebuah model layanan yang memungkinkan pengguna membuat aplikasi yang bergantung pada platform tersebut. Pengguna dan penyedia layanan cloud bertanggung jawab atas langkah-langkah keamanan lapisan platform. Sementara penyedia layanan cloud mengambil tindakan keamanan tambahan, pelanggan bertanggung jawab atas keamanan aplikasi dan lingkungan operasi mereka. Jika platform menggunakan aplikasi pihak ketiga, pihak ketiga tersebut bertanggung jawab atas keamanan aplikasi tersebut. Dalam hal ini, klien mendapatkan informasi sebanyak mungkin dari pihak ketiga untuk menilai risiko dan meningkatkan keamanan data mereka. Terakhir, keamanan infrastruktur IaaS yang merujuk pada infrastruktur sebagai layanan tersedia.

Dengan menggunakan teknologi virtualisasi, model layanan ini menyediakan infrastruktur komputasi awan yang sangat terukur dan terotomatisasi untuk pengguna. Dengan demikian, pengguna dapat membeli sumber daya sesuai permintaan tanpa harus membeli semua perangkat keras. Pelanggan memiliki kontrol keamanan yang lebih besar dalam model layanan ini. Pelanggan bertanggung jawab bersama dengan penyedia layanan cloud untuk keamanan lapisan sumber daya komputasi tervirtualisasi serta sistem operasi, lingkungan runtime, dan aplikasi yang digunakan. Ini mencakup keamanan dan keandalan operasi, pembaruan, dan konfigurasi sumber daya komputasi ini. Pada gilirannya, penyedia layanan cloud bertanggung jawab atas keamanan monitor mesin virtual dan sumber daya yang mendasarinya. Selain itu, karena teknologi virtualisasi komputasi elastis merupakan inti dari IaaS, keamanan virtualisasi termasuk keamanan perangkat lunak virtualisasi dan server virtual sangat penting untuk menjaga aplikasi IaaS aman. Ketiga, jumlah besar pengguna yang dapat diidentifikasi dalam

model komputasi awan, otentikasi diperlukan untuk memastikan bahwa sumber daya atau data pengguna sendiri, dll., tidak disalahgunakan oleh penyedia awan atau pihak lain. Salah satu solusi saat ini adalah menggunakan struktur otentikasi pihak ketiga dengan otoritas sertifikasi yang memberi kedua belah pihak kunci privat untuk mencapai perlindungan privasi dan keamanan data. Keempat, pendekatan responsif untuk keamanan komputasi awan untuk bisnis e-commerce perusahaan e-commerce dapat menggunakan layanan komputasi awan dengan lebih aman dengan menggunakan strategi yang efektif. Strategi-strategi ini termasuk memilih penyedia komputasi awan secara rasional, menerapkan komputasi awan secara logis, mengawasi operasinya, dan menarik diri dari komputasi awan. Pilih penyedia layanan komputasi awan adalah pilihan yang masuk akal.

Pertama, pertimbangkan beberapa faktor untuk memilih penyedia layanan cloud. Untuk memastikan keamanan data dan bisnis, Anda harus memilih penyedia layanan cloud yang telah lulus tinjauan keamanan. Faktor-faktor berikut harus dipertimbangkan saat memilih penyedia layanan cloud: latar belakang penyedia layanan cloud, kemampuan layanan penyedia layanan cloud (termasuk model layanan, model penerapan, dll.), Arsitektur jaringan yang menjadi dasar platform komputasi awan (termasuk metode akses jaringan, jalur transmisi data, dll.) dan kemampuan pengembangan khusus, skalabilitas, ketersediaan, portabilitas, dan interoperabilitas platform komputasi awan, penggunaan sumber daya platform komputasi awan, penyewaan lebar pita, pengawasan, pelatihan, dan biaya lain dari metode penagihan dan standar, kemampuan keamanan penyedia layanan awan (termasuk keamanan lingkungan fisik, kemampuan kontrol akses, kemampuan manajemen konfigurasi, kemampuan perlindungan sistem dan komunikasi, tanggap darurat, dan kemampuan pemulihan cadangan bencana, dll.), kemampuan manajemen keamanan penyedia layanan cloud, dan insiden keamanan serta kerugian yang disebabkan oleh kompensasi penyedia layanan cloud terhadap kemampuan dan standar. Kedua, evaluasi latar belakang karyawan. Perusahaan e-commerce menentukan apakah mereka perlu melakukan pemeriksaan latar belakang pada karyawan penyedia layanan cloud yang mengakses data dan bisnis berdasarkan sensitivitas informasi dan bisnis.

Ketiga, pertimbangan keamanan terkait kontrak layanan. Perusahaan e-commerce harus memperhatikan instruksi privasi yang diberikan oleh penyedia layanan cloud untuk memastikan bahwa penyedia layanan cloud memiliki standar manajemen data yang tinggi. Kontrak layanan yang ditandatangani oleh penyedia layanan cloud harus mencakup ketentuan yang jelas tentang tanggung jawab dan kewajiban penyedia layanan cloud, serta perjanjian tingkat layanan, perjanjian kerahasiaan, dan perjanjian keamanan informasi. Bagaimana dengan penggunaan layanan komputasi awan yang didasarkan pada penelitian ilmiah?

Perusahaan e-commerce harus terlebih dahulu membuat rencana penerapan layanan komputasi awan dengan penyedia layanan cloud. Rencana ini harus dilampirkan pada kontrak.

Perusahaan e-commerce harus mempertimbangkan persyaratan keamanan data dan kelangsungan bisnis saat melakukan migrasi sistem bisnis yang sedang berjalan ke platform komputasi awan. Layanan komputasi awan sendiri atau dipercayakan harus diuji untuk kinerja, fungsi, dan keamanan, dan indikatornya harus memenuhi persyaratan sebelum dioperasikan. Pengawasan pengoperasian layanan komputasi awan. Pertama, perusahaan e-commerce harus memantau pengoperasian penyedia layanan komputasi awan serta penggunaan, manajemen, dan tindakan teknis mereka sendiri. Hal ini dilakukan untuk memastikan bahwa kontrak layanan yang ditandatangani dengan penyedia layanan komputasi awan mematuhi tanggung jawab dan kewajiban yang ditetapkan dan untuk memastikan bahwa kualitas layanan memenuhi persyaratan kontrak dan standar teknis. Kedua, penting untuk menjelaskan tanggung jawab perusahaan e-commerce dan penyedia layanan cloud. Regulasi perusahaan e-commerce meliputi pelanggaran kontrak, tindakan keamanan, dll. Regulasi penyedia layanan cloud meliputi status operasional, perubahan besar, pengawasan peristiwa keamanan, dll.

Penarikan diri dari layanan komputasi awan: Anda harus keluar dari layanan komputasi awan ketika kontrak berakhir atau ketika data dan sistem bisnis dimigrasikan ke platform komputasi awan lainnya. Penarikan diri dari layanan komputasi awan adalah proses yang rumit yang melibatkan persyaratan, tanggung jawab, dan kewajiban, pengembalian data pengguna, ketersediaan dan kelangsungan bisnis, sumber daya fisik, dan hak akses. Perusahaan e-commerce harus menentukan batas serah terima data, memverifikasi keamanan data, menghapus data dengan aman, dan sebagainya.

(5) Perlindungan keamanan blockchain

Pada dasarnya, blockchain adalah database buku besar yang dapat diakses secara terdesentralisasi. Jaringan blockchain tidak memiliki node pusat, dan semua node memiliki status yang sama. Blockchain dapat dibagi menjadi rantai publik, rantai koalisi, dan rantai pribadi berdasarkan cara mereka diakses. Rantai publik sepenuhnya terdesentralisasi, memungkinkan setiap individu atau kelompok untuk mengirim transaksi, dan merupakan yang paling awal dan paling banyak digunakan. Rantai koalisi juga terdesentralisasi sebagian, dengan beberapa node yang telah dipilih sebelumnya ditetapkan sebagai pemegang buku dalam sebuah grup.

Pembukuan rantai pribadi hanya menggunakan teknologi buku besar blockchain, dan mereka hanya dapat ditulis oleh organisasi atau individu yang memiliki akses eksklusif ke blockchain. Dimungkinkan untuk digunakan secara luas, data yang tidak dapat dirusak, tidak

dapat dipalsukan, dan diverifikasi berkat teknologi unik yang digunakan dalam blockchain. Akan tetapi, dalam operasi blockchain yang sebenarnya, ada masalah keamanan seperti serangan aritmatika 51% (sebuah node yang jahat dapat memiliki kontrol atas 51% kekuatan aritmatika seluruh jaringan), bug perangkat lunak, kebocoran privasi, dan lainnya.

Karena bursa mata uang digital memiliki banyak mata uang digital, mereka cocok untuk peretas. Pemrosesan bahasa alami, visi komputer, pembelajaran mendalam, robotika, dan pengenalan suara adalah bidang penelitian kecerdasan buatan (AI). Kecerdasan buatan diharapkan akan mengubah banyak hal dalam e-commerce, seperti pencarian dan pengenalan gambar visual, rekomendasi produk, bantuan cerdas, dan perlindungan jaringan e-commerce. Selain itu, AI dapat mendeteksi virus dan kode program berbahaya dengan leb Sebagai contoh, serangan-serangan berikut dilakukan melalui penggunaan kecerdasan buatan. Pertama, meniru perilaku manusia, seperti menggunakan bot web, nomor telepon, dan alamat IP ilegal yang mungkin terlibat dalam perilaku curang, dan melanggar otentikasi jaringan melalui pengenalan gambar dan suara untuk melakukan serangan, dll. Kedua, serangan pengujian fuzzy AI.

Pengujian fuzzy AI adalah metode yang efektif untuk melakukan pengujian perangkat lunak dan penambangan kerentanan, dan penguji profesional dapat menggunakannya untuk menemukan kerentanan umum dan kerentanan zero-day dalam sistem. Namun, penyerang dapat menggunakan pembelajaran mesin untuk mengotomatiskan prosedur pengujian fuzzy untuk menemukan kerentanan sistem dengan cepat, yang mengakibatkan peningkatan serangan terhadap sistem dan pembelajaran mesin. Teknik yang sama untuk menemukan masalah sistem dan menambalnya pada tahap awal adalah pendekatan perlindungan keamanan yang tepat.

Ketiga, serangan Deepfake. Deepfake adalah teknik yang menggunakan kecerdasan buatan untuk mensintesis gambar, suara, dan gambar yang sangat mirip dengan kenyataan. Generative Adversary Networks (GAN) dapat melakukannya dengan melatih jaringan saraf dengan data yang berlawanan, sehingga gambar dapat dibuat atau dirusak secara otomatis. Sebagai contoh, ketika suara kecil dimasukkan ke dalam gambar panda, itu dianggap sebagai owa. Penyerang memaksa kendaraan ke dalam kondisi mengemudi yang tidak normal dengan rambu jalan atau rintangan yang menipu sistem pengambilan keputusan di area tanpa pengemudi. Salah satu cara terbaik untuk melindungi keamanan adalah dengan menggunakan video anti-pengeditan yang menggunakan teknologi watermarking yang dipelajari secara menyeluruh. Teknologi ini dapat mengidentifikasi apakah gambar dan suara telah diubah secara ilegal melalui integritas watermark. Keempat, serangan keracunan data. Pembelajaran mesin, pembelajaran mendalam, dan algoritme kecerdasan buatan lainnya sangat bergantung pada kualitas data yang digunakan untuk pelatihan. Akibatnya, data pelatihan dapat terkontaminasi atau diracuni dengan

mengubah kumpulan data pelatihan atau membuang sampel berbahaya yang dibuat dengan hati-hati selama pelatihan model. Ini mengganggu pelatihan model pembelajaran mesin dan mengurangi keakuratan model yang dihasilkan. Menjaga kerahasiaan algoritme model yang sesuai dan mengawasi data pelatihan secara ketat adalah metode perlindungan yang tepat:

Kelima, kegagalan untuk mengekstraksi model serangan ini adalah penyerang yang memiliki akses black-box tetapi tidak memahami parameter model atau data pelatihan, sehingga mereka bertujuan untuk mencuri model. Serangan percobaan digunakan oleh penyerang untuk mendapatkan parameter model target atau membuat model alternatif, juga dikenal sebagai model bayangan, yang memiliki fungsi yang sebanding dengan model dengan membuat permintaan untuk memulai kueri ke layanan target. Mengurangi keakuratan penyerang untuk mendapatkan model adalah strategi keamanan yang tepat.

(6) Perlindungan keamanan kecerdasan buatan

Pemrosesan bahasa alami, visi komputer, pembelajaran mendalam, robotika, dan pengenalan suara adalah bidang penelitian kecerdasan buatan (AI). Faktor-faktor seperti pencarian visual dan pengenalan gambar, rekomendasi produk, bantuan cerdas, dan lainnya seharusnya diubah oleh kecerdasan buatan dalam e-commerce. AI dapat digunakan untuk mendeteksi virus dan kode program berbahaya dengan lebih baik saat melakukan perlindungan keamanan jaringan e-commerce, memantau dan mengurai log, mengotentikasi pengguna secara terus menerus, dll. Namun, AI juga dapat digunakan untuk mengancam keamanan siber bisnis elektronik. Sebagai contoh, serangan-serangan berikut dilakukan melalui penggunaan kecerdasan buatan.

Pertama, meniru perilaku manusia, seperti menggunakan bot web, nomor telepon, dan alamat IP ilegal yang mungkin terlibat dalam perilaku curang, dan melanggar otentikasi jaringan melalui pengenalan gambar dan suara untuk melakukan serangan, dll. Kedua, serangan pengujian fuzzy AI. Pengujian fuzzy AI adalah metode yang efektif untuk melakukan pengujian perangkat lunak dan penambangan kerentanan, dan penguji profesional dapat menggunakannya untuk menemukan kerentanan umum dan kerentanan zero-day dalam sistem. Namun, penyerang dapat menggunakan pembelajaran mesin untuk mengotomatiskan prosedur pengujian fuzzy untuk menemukan kerentanan sistem dengan cepat, yang mengakibatkan peningkatan serangan terhadap sistem dan pembelajaran mesin. Teknik yang sama untuk menemukan masalah sistem dan menambalnya pada tahap awal adalah pendekatan perlindungan keamanan yang tepat. Ketiga, serangan Deepfake. Deepfake adalah istilah yang mengacu pada metode yang menggunakan kecerdasan buatan untuk menggabungkan suara, gambar, dan gambar yang tampak sangat nyata. Dengan melatih jaringan saraf dengan data

yang berlawanan, Generative Adversary Networks (GAN) memungkinkan penggunaan Deepfake. Dengan demikian, gambar dapat dihasilkan atau dirusak secara otomatis. Sebagai contoh, ketika suara kecil dimasukkan ke dalam gambar panda, itu dianggap sebagai owa. Penyerang memaksa kendaraan ke dalam kondisi mengemudi yang tidak normal dengan rambu jalan atau rintangan yang menipu sistem pengambilan keputusan di area tanpa pengemudi.

Salah satu cara terbaik untuk melindungi keamanan adalah dengan menggunakan video anti-pengeditan yang menggunakan teknologi watermarking yang dipelajari secara menyeluruh. Teknologi ini dapat mengidentifikasi apakah gambar dan suara telah diubah secara ilegal melalui integritas watermark. Keempat, serangan keracunan data. Pembelajaran mesin, pembelajaran mendalam, dan algoritme kecerdasan buatan lainnya sangat bergantung pada kualitas data yang digunakan untuk pelatihan. Akibatnya, data pelatihan dapat terkontaminasi atau diracuni dengan mengubah kumpulan data pelatihan atau membuang sampel berbahaya yang dibuat dengan hati-hati selama pelatihan model. Ini mengganggu pelatihan model pembelajaran mesin dan mengurangi keakuratan model yang dihasilkan.

Menjaga kerahasiaan algoritme model yang sesuai dan mengawasi data pelatihan secara ketat adalah metode perlindungan yang tepat. Kelima, kegagalan untuk mengekstraksi model serangan ini dilakukan oleh penyerang yang memiliki akses black-box tetapi tidak memahami data pelatihan atau parameter model. Untuk mencuri parameter model target, penyerang menggunakan serangan percobaan untuk membuat model alternatif, juga disebut model bayangan, yang memiliki fungsi yang mirip dengan model dengan membuat permintaan untuk memulai kueri ke layanan target. Mengurangi keakuratan penyerang untuk mendapatkan model adalah strategi keamanan yang tepat.

5.3.3 Langkah-Langkah Regulasi

Berikut ini terutama membahas langkah-langkah normatif dari beberapa elemen: organisasi yang berkaitan dengan keamanan jaringan, sistem manajemen keamanan jaringan, dan undang-undang dan peraturan yang berkaitan dengan keamanan internet.

1. Organisasi terkait keamanan siber

(1) Standarisasi keamanan siber dan organisasi terkait manajemen sumber daya

Pertama, organisasi yang berkaitan dengan standardisasi internasional dan manajemen sumber daya. Organisasi Internasional untuk Standardisasi (ISO), Tim Teknik Internet (IETF), Otoritas Nomor Ditetapkan Internet (IANA), dan Internet Corporation for Assigned Names and Numbers (ICANN) adalah beberapa organisasi yang terlibat dalam topik ini. ISO juga telah mengembangkan model referensi Open Systems Interconnection (OSI) dan a semua

mekanisme ini berkaitan dengan layanan keamanan. Misalnya, mekanisme enkripsi berkaitan dengan layanan kerahasiaan data, mekanisme integritas data berkaitan dengan layanan integritas data, dan sebagainya.

IETF (IETF) adalah kelompok internasional terbuka yang tugas utamanya adalah mengembangkan dan merumuskan standar teknis yang terkait dengan Internet. IETF juga memperhatikan masalah keamanan Internet dan telah menerbitkan serangkaian memorandum, Request for Comments (RFC). RFC telah memainkan peran penting dalam meningkatkan dan memperbaiki keamanan Internet, seperti dalam langkah penting menuju tata kelola bersama Internet di seluruh dunia, Amerika Serikat memindahkan fungsi IANA ke komunitas pemangku kepentingan Internet global pada tahun 2016.

Internet Corporation for Assigned Names and Numbers (ICANN) bertanggung jawab atas alokasi alamat Protokol Internet (IP), pemberian pengenal protokol, pengelolaan sistem generic top-level domain (gTLD) dan sistem top-level domain negara dan regional (ccTLD), dan pengelolaan sistem root server. ICANN juga mengatur dan mengelola berbagai komponen teknis Layanan Nama Domain (DNS) untuk memastikan bahwa semua pengguna Internet dapat menemukan alamat yang benar. Aturan transaksi keuangan, kontrol konten web, email komersial spontan (spam), dan perlindungan data adalah masalah keamanan siber lainnya yang berada di luar tanggung jawab koordinasi ICANN. Kedua, lembaga yang bertanggung jawab atas standarisasi keamanan siber di China. China sangat peduli dengan standarisasi keamanan siber; Komite Teknis Nasional untuk Standarisasi Keamanan Informasi adalah organisasi yang relevan.

(2) Organisasi Koordinasi Keamanan Siber

Terutama, organisasi koordinasi keamanan jaringan bertanggung jawab untuk mengatur dan mengorganisasikan penelitian atau aturan yang relevan tentang keamanan jaringan. Untuk menyelesaikan pekerjaan yang terkait, organisasi koordinasi keamanan yang sesuai telah dibentuk di Cina dan di tingkat internasional. Saat ini, Tim Respons Bencana Computer (CERT/CC) adalah organisasi internasional yang terkenal untuk mengkoordinasikan masalah keamanan Internet. Pekerjaan organisasi ini termasuk menyediakan solusi untuk masalah keamanan, membangun database masalah kerentanan berdasarkan data yang dikumpulkan oleh pengguna Internet untuk menyediakan informasi yang diperlukan anggota dalam.

Di Tiongkok, organisasi yang relevan adalah Pusat Tanggap Darurat Internet Nasional (CNCERT), yang berfungsi sebagai unit utama dalam sistem tanggap darurat jaringan komputer negara tersebut. Tanggung jawab utamanya adalah melakukan pencegahan, deteksi, peringatan dini, dan pembuangan insiden keamanan jaringan Internet yang terkoordinasi sesuai

dengan prinsip "pencegahan aktif, deteksi tepat waktu, respons cepat, dan pemulihan". Platform Berbagi Kerentanan Keamanan Informasi Nasional (CNVD) dioperasikan dan dikelola oleh lembaga ini untuk memastikan bahwa jaringan publik aman dan infrastruktur informasi penting beroperasi dengan aman.

CNCERT membangun Aliansi Antivirus China (ANVA) dan Aliansi Tata Kelola Ancaman Keamanan Jaringan Internet China (CCTGA). Kedua kelompok ini bekerja sama dalam masalah keamanan jaringan di seluruh dunia dan berkomitmen untuk membangun mekanisme pembuangan dan respons yang cepat untuk insiden keamanan jaringan yang terjadi di seluruh dunia.

2. Organisasi terkait keamanan siber

Perusahaan e-commerce harus membuat organisasi manajemen keamanan jaringan dan menetapkan undang-undang dan peraturan untuk menjaga keamanan jaringan mereka. Sistem terkait manajemen keamanan jaringan terutama mencakup strategi manajemen keamanan jaringan, sistem manajemen keamanan jaringan, sistem manajemen otorisasi dan persetujuan, komunikasi dan kerja sama, sistem audit dan inspeksi, dll. Strategi kalender gantung keamanan jaringan yang efektif adalah salah satu komponen yang paling penting.

Perusahaan e-commerce harus membangun sistem manajemen keamanan yang sesuai untuk semua jenis konten manajemen yang terlibat dalam aktivitas manajemen keamanan jaringan, seperti prosedur operasi, perawatan darurat, pemeliharaan harian, penyimpanan file perangkat keras dan perangkat lunak, kerahasiaan informasi, manajemen otoritas, dll. Perusahaan e-commerce harus jelas menunjukkan masalah persetujuan, departemen persetujuan, dan pemberi persetujuan dengan tanggung jawab masing-masing departemen dan posisi. Prosedur persetujuan dibuat untuk hal-hal seperti perubahan sistem, operasi penting, akses fisik ke sistem, dll., dan masalah persetujuan ditinjjau. Dengan cepat, pemberi persetujuan dan departemen persetujuan memberikan informasi tentang hal-hal yang memerlukan persetujuan dan otorisasi.

Sistem komunikasi dan kerja sama memungkinkan berbagai jenis manajer, lembaga pemerintah, dan departemen manajemen keamanan jaringan perusahaan e-commerce untuk berkomunikasi satu sama lain dan bekerja sama untuk memecahkan masalah keamanan jaringan. Mereka juga mengatur pertemuan teratur untuk mendorong kerja sama. Selain itu, kerja sama dan komunikasi dengan organisasi keamanan, pakar industri, dan pemasok harus ditingkatkan. Daftar kontak unit penjangkauan harus dibuat untuk mempermudah komunikasi dan pertukaran. Daftar ini harus mencakup informasi seperti nama unit penjangkauan, konten kerja sama, narahubung, dan informasi kontak lainnya. Perusahaan e-commerce membuat

laporan pemeriksaan keamanan dengan menggunakan sistem audit dan inspeksi. Pemeriksaan rutin keamanan termasuk operasi harian, kerentanan sistem dan pencadangan data; pemeriksaan keamanan menyeluruh secara teratur, termasuk konsistensi konfigurasi dan kebijakan keamanan, penerapan sistem manajemen keamanan, dll.

Untuk sistem manajemen keamanan yang disebutkan di atas, departemen atau individu tertentu harus ditunjuk atau diberi wewenang untuk bertanggung jawab secara formal dan efektif untuk mengembangkan dan mengeluarkan sistem tersebut, serta untuk mengontrol versinya. Setelah membangun sistem manajemen jaringan, perlu untuk secara teratur memvalidasi dan menegaskan bahwa itu sesuai dan diterapkan, serta merevisi setiap kelemahan atau area yang perlu ditingkatkan.

3. Hukum dan peraturan terkait keamanan jaringan

Berikut ini adalah penjelasan tentang undang-undang dan peraturan keamanan jaringan Tiongkok. Ini membantu mengamankan jaringan e-commerce di tingkat hukum. jaringan komputer, pengelolaan pencegahan dan pengendalian virus komputer, dan pengelolaan kepatuhan data privasi.

(1) Hukum dan peraturan tentang keamanan jaringan

Pertama, Langkah-langkah Administratif untuk Perlindungan Keamanan Jaringan Internasional Jaringan Informasi Komputer. Langkah-langkah ini disetujui oleh Dewan Negara pada tanggal 11 Desember 1997, dikeluarkan oleh Kementerian Keamanan Publik pada tanggal 30 Desember 1997, dan dimulai pada tanggal 30 Desember 1997. Tujuan pengembangan "Langkah-langkah" dijelaskan dalam Pasal 1 "Langkah-langkah". Tujuannya adalah untuk meningkatkan keamanan jaringan informasi komputer internasional untuk menjaga ketertiban umum dan stabilitas sosial. Metode ini berlaku untuk jaringan internasional dan mencakup manajemen perlindungan keamanan jaringan informasi komputer Republik Rakyat Tiongkok, seperti yang dijelaskan dalam Pasal 2 dari "Langkah-langkah". Objektif yang relevan. Pengguna jaringan informasi komputer serta entitas dan individu yang terlibat dalam bisnis jaringan internasional dijelaskan dalam Pasal 3 dari "Langkah-langkah".

Isi utama: "Langkah-langkah" dari Pasal 4-8 dan Pasal 10 memberikan tanggung jawab utama untuk perlindungan keamanan jaringan informasi komputer, termasuk departemen, unit, dan individu yang relevan. "Langkah-langkah" dari Pasal 3, Pasal 17, dan Pasal 19 menjelaskan tugas dan kewajiban organ keamanan publik, dan "Langkah-langkah" dari Pasal 20–23 dengan tegas menetapkan perlunya memikul tanggung jawab hukum atas pelanggaran ini. Kedua, Keputusan Komite Tetap Kongres Rakyat Nasional tentang Perlindungan Keamanan Internet diadopsi pada pertemuan ke-19 Komite Tetap Kongres Rakyat Nasional Kesembilan pada

tanggal 28 Desember 2000 direvisi pada tahun 2011. Tujuan: Keputusan ini bertujuan untuk mendorong pertumbuhan Internet yang sehat di Tiongkok dengan menjaga keamanan nasional dan kepentingan sosial masyarakat serta melindungi hak dan kepentingan yang sah dari individu, badan hukum, dan organisasi lain dengan meningkatkan keuntungan dan menghilangkan pelanggaran. Keputusan ini mendefinisikan tindakan ilegal berdasarkan Internet dalam Pasal 1-4. Menentukan aturan untuk kejahatan Internet. Pasal 5-7 Keputusan tersebut dengan jelas menyatakan aturan untuk kejahatan internet ilegal. Ketiga, Undang-Undang Keamanan Jaringan Republik Rakyat Tiongkok. Pada tanggal 7 November 2016, Komite Tetap Kongres Rakyat Nasional Kedua Belas memutuskan untuk mengadopsi Undang-Undang Keamanan Siber Republik Rakyat Tiongkok (juga dikenal sebagai Undang-Undang Keamanan Siber). Itu diundangkan oleh Keputusan Presiden No. 53 Republik Rakyat Tiongkok, dan mulai berlaku pada tanggal 1 Juni 2017.

Tujuan, serta status hukum pasal 1 UU Keamanan Siber adalah undang-undang dasar pertama di China yang secara komprehensif mengatur masalah siber. Undang-undang ini menetapkan tujuan untuk melindungi keamanan siber, menjaga keamanan dunia maya dan kedaulatan nasional, kepentingan sosial masyarakat, melindungi hak-hak dan kepentingan sah warga negara, badan hukum, dan organisasi lain, dan mendorong pengembangan informatisasi ekonomi dan sosial yang sehat. Ketika digunakan pasal 2 Undang-Undang Keamanan Siber menetapkan bahwa pembangunan, pengoperasian, pemeliharaan, dan penggunaan jaringan di Republik Rakyat Tiongkok, serta pengawasan dan pengelolaan keamanan jaringan, harus diatur oleh Undang-Undang ini. Pasal 77 menetapkan bahwa, selain Undang-Undang ini, operasi dan perlindungan keamanan jaringan yang menyimpan dan memproses informasi yang melibatkan rahasia negara juga harus sesuai dengan ketentuan undang-undang dan peraturan administratif terkait lainnya. Istilah-istilah yang terkait. Istilah-istilah yang berkaitan dengan keamanan jaringan didefinisikan dalam Pasal 76 "Hukum Keamanan Jaringan".

Di antaranya, "jaringan" adalah istilah yang mengacu pada komputer atau terminal informasi lainnya dan peralatan terkait yang terdiri dari aturan dan prosedur tertentu untuk pengumpulan, penyimpanan, transmisi, pertukaran, dan pemrosesan sistem informasi. Keamanan jaringan juga mengacu pada kemampuan untuk melindungi jaringan dari serangan, gangguan, kerusakan, dan penggunaan jaringan secara tidak sah. Data jaringan mengacu pada semua jenis data elektronik yang dikumpulkan, disimpan, dikirim, diproses, atau dibuat melalui jaringan. Informasi pribadi mengacu pada semua jenis data yang direkam secara elektronik atau dengan cara lain yang dapat mengidentifikasi identitas seseorang, baik secara terpisah maupun bersamaan dengan informasi lain. Contoh informasi pribadi termasuk namun tidak

terbatas pada nama, tanggal lahir, nomor kartu identitas, alamat email, alamat IP, dan informasi lainnya. Fokus utama Pertama, undang-undang ini menetapkan dasar untuk kedaulatan siber Tiongkok. Pasal 1 UU Keamanan Siber menjelaskan prinsip kedaulatan di dunia maya, Pasal 3 menjelaskan bahwa keamanan siber dan pengembangan informasi sama penting, dan Pasal 4-7 dan 12–20 menjelaskan bagaimana koordinasi pemerintah dan tata kelola bersama penting.

Kedua, UU Keamanan Jaringan menjelaskan kewajiban dan tanggung jawab keamanan operator jaringan, produk jaringan, dan penyedia layanan jaringan. Pasal 9-11 dan 21-29 jelas menetapkan kewajiban dan tanggung jawab keamanan operator jaringan, produk jaringan, dan penyedia layanan jaringan, dan jika pihak-pihak yang bertanggung jawab tidak mematuhi ketentuan yang relevan, mereka akan menghadapi risiko hukum. Ketiga, langkah-langkah pengaturan yang jelas dan otoritas pengatur.

Pertama-tama, jelas bahwa keamanan jaringan ditanggung oleh departemen regulasi pemerintah dan fungsi yang terkait. Menurut Pasal 8, departemen informasi Internet negara bertanggung jawab untuk mengatur keamanan jaringan serta tugas pengawasan dan manajemen terkait. Dalam bidang tanggung jawab masing-masing, departemen telekomunikasi Dewan Negara, departemen keamanan publik, dan otoritas terkait lainnya sesuai dengan undang-undang ini, undang-undang ini, dan peraturan administratif yang relevan bertanggung jawab atas perlindungan keamanan jaringan serta pengawasan dan pekerjaan manajemen. Departemen terkait dari pemerintah daerah setempat pada atau di atas tingkat kabupaten bertanggung jawab atas perlindungan keamanan jaringan serta pekerjaan manajemen. Kedua, perlindungan infrastruktur kritis dan informasi. Pasal 31–39 menetapkan sistem perlindungan keamanan infrastruktur informasi penting, dan Pasal 30–40 membahas persyaratan rilis informasi jaringan, dan kemudian meningkatkan perlindungan informasi pribadi.

Di antaranya, Pasal 38 memberikan penjelasan tentang prosedur kontrol operator dalam hal ini, dan Pasal 39 memberikan penjelasan tentang prosedur pengawasan pemerintah dalam hal ini. Pasal 50 menjelaskan tanggung jawab departemen pengawasan pemerintah untuk visi dan prosedur pengawasan keamanan informasi, dan Pasal 43 menjelaskan hak para pihak untuk mengawasi informasi pribadi. Dalam bagian keempat, diberikan penjelasan tentang apa yang harus dilakukan oleh individu, organisasi, dan perlindungan keamanan jaringan industri. Pasal 11 dan 12 membahas tanggung jawab individu, organisasi, dan keamanan jaringan industri, dan pasal 17–20 membahas cara membangun sistem layanan sosial keamanan jaringan, metode manajemen yang inovatif untuk keamanan jaringan, dan pengawasan dan dukungan untuk pendidikan dan pelatihan keamanan. Kelima, membangun pemantauan keamanan jaringan yang lebih lengkap dan terintegrasi, serta mekanisme untuk tanggap darurat, peringatan dini,

dan pemberitahuan. Negara membentuk sistem pemantauan keamanan jaringan dan peringatan dini serta pemberitahuan informasi sesuai dengan Pasal 51 dan Pasal 52.

Departemen yang bertanggung jawab atas perlindungan keamanan infrastruktur informasi harus membangun dan meningkatkan industri, bidang pemantauan keamanan jaringan dan sistem peringatan dini dan pemberitahuan informasi sesuai dengan ketentuan pemantauan keamanan jaringan dan informasi peringatan dini dan pemberitahuan informasi. Mekanisme kerja tanggap darurat dan penilaian risiko keamanan jaringan dibahas dalam artikel 53–58. Tanggung jawab hukum diperjelas. Pasal 59-75 dari "Hukum Keamanan Jaringan" meningkatkan hukuman atas pelanggaran hukum dan memperjelas siapa yang bertanggung jawab atas pelanggaran ini.

(2) Hukum dan peraturan tentang manajemen pencegahan dan pengendalian virus

Pada tanggal 26 April 2000, komputer Kementerian Keamanan Publik mengeluarkan "Manajemen Manajemen Pencegahan dan Pengendalian Virus Komputer", yang mencakup tujuh elemen berikut. Pertama-tama, virus komputer dikenali. Virus komputer dibuat atau dimasukkan ke dalam program komputer untuk merusak fungsi atau menghancurkan data, mengganggu penggunaan komputer, dan dapat mereplikasi sendiri serangkaian instruksi atau kode program. Kedua, Pasal 5, 6, dan 12 dari pendekatan ini mengatur perilaku orang untuk menghindari bahaya virus komputer. Ketiga, Pasal 11 dari pendekatan ini menjelaskan bagaimana unit sistem informasi komputer yang terlibat dalam pencegahan dan pengendalian virus komputer harus melakukan tugastugas tersebut. Keempat, Pasal 8, 13, dan 14 dari pendekatan ini menjelaskan persyaratan unit produksi yang terlibat dalam produk pencegahan dan pengendalian virus komputer.

Pasal 4 dan 15 dari bagian kelima memberikan penjelasan tentang peran organ keamanan publik dalam pencegahan dan pengendalian virus komputer oleh otoritas terkait. Pasal 6, 7, 10, dan 21 mengatur virus komputer dan penyebaran epidemi. Ketujuh, Pasal 15–20 dari langkah-langkah ini memberikan penjelasan tentang konsekuensi dari pelanggaran yang berkaitan dengan virus komputer.

(3) Hukum dan peraturan tentang manajemen kepatuhan privasi data

Saat ini, ada lebih banyak standar dan norma yang berkaitan dengan data besar dan akan terus diperkenalkan, bersama dengan kebutuhan untuk pengawasan lintas batas pada aliran data lintas batas, manajemen kepatuhan privasi data adalah cara penting untuk mengurangi risiko data besar. Pertama, undang-undang dan peraturan tentang kepatuhan privasi data di Amerika Serikat dan Eropa. Undang-undang terpenting tentang kepatuhan privasi data di Amerika Serikat termasuk Fair Credit Reporting Act tahun 1970, Privacy Act tahun 1974, Electronic

Communications Privacy Act tahun 1986, dan Children's Online Privacy Protection Act tahun 1998. Selain itu, Undang-Undang Hak Privasi Konsumen AS dikeluarkan pada Februari 2012, yang mengatakan bahwa pengguna Internet harus memiliki kendali atas data pribadi yang dikumpulkan dan digunakan, dan bahwa perusahaan harus mematuhi standar transparansi dan kewajaran tujuan saat menangani data pribadi.

Pada tahun 1995, Uni Eropa (UE) membuat Petunjuk tahun 1995 tentang Perlindungan Hak-hak Individu sehubungan dengan Pemrosesan Data Pribadi dan Pemindahan Data Pribadi secara Bebas (Petunjuk Perlindungan Data) menetapkan standar minimum untuk perlindungan data pribadi. Pada bulan Januari 2012, Komisi Eropa mengajukan Peraturan Perlindungan Data Umum (GDPR) yang baru. Peraturan ini menetapkan konsep ini terdiri dari empat pilar. Pertama, Petunjuk Perlindungan Data harus digunakan untuk menyamakan undang-undang perlindungan data di seluruh Eropa dan mengubah undang-undang nasional. Kedua, undang-undang perlindungan data Uni Eropa harus diterapkan oleh perusahaan yang memproses data pribadi warga negara Uni Eropa. Ketiga, untuk memberikan hak untuk dilupakan yaitu, jika tidak ada alasan hukum untuk menyimpannya individu memiliki hak untuk meminta penghapusan data yang melibatkan privasi mereka, termasuk tautan ke data pribadi yang disediakan oleh penyedia layanan pencarian Internet. Keempat, untuk mekanisme pemrosesan regulator perlindungan data tunggal, yang akan memberikan pemahaman kepada individu dan perusahaan. Selain Brasil, Jepang, dan Korea Selatan mengeluarkan Undang-Undang Perlindungan Informasi Pribadi, Peraturan Perlindungan Data Umum, yang diadopsi pada tahun 2016 dan mulai berlaku pada bulan Mei 2018, memperketat perlindungan data pribadi warga negara anggota Uni Eropa lebih dari Petunjuk Perlindungan Data. Kedua, undang-undang Cina tentang manajemen kepatuhan privasi data terdiri dari "dokumen peraturan umum+ industri dan peraturan dan regulasi lokal".

Keputusan Komite Tetap Kongres Rakyat Nasional tentang Penguatan Perlindungan Informasi Jaringan diadopsi pada pertemuan ke-30 Komite Tetap Kongres Rakyat Nasional ke-11 pada tanggal 28 Desember 2012. Keputusan ini memperkuat perlindungan hukum atas informasi pribadi warga negara, mendefinisikan peran dan tanggung jawab penyedia layanan jaringan, dan memberikan perangkat peraturan yang diperlukan kepada departemen pemerintah yang berwenang. Rencana Aksi untuk Mempromosikan Pengembangan Data Besar yang dikeluarkan oleh Dewan Negara pada bulan Agustus 2015 menunjukkan bahwa membangun sistem manajemen keamanan data besar diperlukan. Rencana tersebut menjelaskan batas-batas ruang lingkup, subjek yang bertanggung jawab, dan persyaratan khusus untuk perlindungan keamanan jaringan di semua aspek pengumpulan, trans-misi, penyimpanan, penggunaan, dan

pembukaan data. Rencana juga menunjukkan bahwa sistem manajemen keamanan dan kerahasiaan yang diperlukan untuk menjaga keamanan dan amandemen (IX) Hukum Pidana Republik Rakyat Tiongkok mulai berlaku pada tahun 2015. Ini mengubah hukuman untuk kejahatan yang berkaitan dengan pelanggaran informasi pribadi warga negara (Pasal 253-1).

Undang-Undang Keamanan Siber, yang secara resmi diterapkan pada tanggal 1 Juni 2017, mengadopsi bab khusus dalam bentuk undang-undang dasar nasional untuk membuat ketentuan umum tentang keamanan informasi jaringan, menetapkan tujuan umum dan prinsip-prinsip dasar keamanan informasi jaringan, memperjelas norma dan hukuman umum untuk pengumpulan dan penggunaan informasi pribadi oleh operator jaringan, membangun sistem kerahasiaan informasi jaringan dan melindungi hak privasi subjek jaringan, membentuk organ administratif untuk prosedur dan sistem pengawasan keamanan informasi jaringan, memberikan hukuman dan langkah-langkah pemberantasan kejahatan keamanan informasi jaringan, dll. Dapat dilihat bahwa "Undang-Undang Keamanan Jaringan" dengan jelas memenuhi kewajiban subjek yang bertanggung jawab atas perlindungan informasi pribadi, yaitu pengumpulan dan penggunaan informasi pribadi operator jaringan termasuk pemilik jaringan, manajer jaringan, dan penyedia layanan jaringan adalah subjek yang bertanggung jawab atas perlindungan informasi pribadi, dan perlu menerima pengawasan dan pengelolaan departemen informasi jaringan negara dan departemen terkait. Undang-undang Keamanan Siber mengimbangi perlindungan yang wajar atas informasi pribadi dan inovasi dalam penggunaan informasi pribadi, secara sistematis mendefinisikan persyaratan untuk perlindungan informasi pribadi, dan mengikuti standar nasional dan internasional. Setiap aspek manajemen Kerangka Kerja Privasi APEC, yang disepakati oleh Kerja Sama Ekonomi Asia Pasifik (APEC) pada tahun 2005, sangat selaras dengan persyaratan Undang-Undang Keamanan Siber yang berkaitan dengan perlindungan informasi pribadi. Ranking yang tinggi untuk Undang-Undang Keamanan Siber menunjukkan komitmen negara untuk memerangi kejahatan informasi secara menyeluruh. Sampai titik tertentu, ini melengkapi undang-undang administratif tentang perlindungan informasi pribadi dan menandai awal yang baru untuk perlindungan informasi pribadi warga negara.

Informasi pribadi individu dilindungi oleh hukum, menurut Pasal 111 Konstitusi Perdata Republik Rakyat Tiongkok, yang berlaku pada tanggal 1 Januari 2021. Setiap organisasi atau individu yang membutuhkan informasi pribadi orang lain harus mematuhi undang-undang saat mengumpulkan, menggunakan, memproses, atau mengirimkan informasi pribadi orang lain. Tidak boleh mengumpulkan, menggunakan, atau mengirimkan informasi pribadi orang lain secara ilegal, atau memperdagangkan, memberikan, atau mengungkapkan informasi pribadi

orang lain. Sesi keempat Kongres Rakyat Nasional ke-13 pada bulan Maret 2021 mengadopsi "Garis Besar Rencana Lima Tahun Keempat Belas untuk Pembangunan Ekonomi dan Sosial Republik Rakyat Tiongkok dan Visi 2035", yang menyatakan bahwa mereka akan memperkuat perlindungan data yang melibatkan kepentingan nasional, rahasia komersial, dan privasi pribadi; mempercepat promosi undang-undang dasar yang berkaitan dengan keamanan data dan perlindungan informasi pribadi; dan meningkatkan perlindungan keamanan data dan informasi pribadi meningkatkan klasifikasi dan sistem perlindungan penilaian yang berlaku untuk lingkungan data besar. Undang-undang Keamanan Data Republik Rakyat Tiongkok, yang diadopsi pada pertemuan ke-29 Komite Tetap Kongres Rakyat Nasional ke-13 pada tanggal 10 Juni 2021, secara efektif mengisi kesenjangan hukum di bidang keamanan data di Tiongkok. Undang-undang tersebut, yang merupakan undang-undang terkait keamanan data pertama di China, akan membawa konstruksi dan pengawasan keamanan data di berbagai industri di China ke era baru yang sesuai dengan hukum dan kepatuhan. Undang-undang tersebut menetapkan persyaratan khusus untuk reformasi dan pembangunan kelembagaan keamanan data, pengawasan dan pengendalian keamanan data, penilaian dan perlindungan keamanan data, dan penetapan siste

Manajemen keamanan termasuk klasifikasi dan manajemen data, penilaian risiko, deteksi, dan peringatan dini serta tanggap darurat, pembangunan mekanisme keamanan untuk berbagi data pemerintah secara terbuka, dan hukuman untuk pelanggaran. Ini juga memperjelas tanggung jawab organisasi dan individu yang melakukan aktivitas data untuk menjaga keamanan data. Memiliki undang-undang ini akan melindungi hak dan kepentingan yang sah dari semua data pribadi dan organisasi. Pada tanggal 20 Agustus 2021, pertemuan ke-30 Komite Tetap Kongres Rakyat Nasional ke-13 mengadopsi Undang-Undang Republik Rakyat Tiongkok tentang Perlindungan Informasi Pribadi, yang berlaku efektif pada tanggal 1 November 2021, yang merupakan undang-undang khusus pertama untuk perlindungan informasi pribadi di Tiongkok.

Undang-undang tersebut secara ketat melindungi hak-hak individu dalam kegiatan pemrosesan informasi pribadi, memperjelas tanggung jawab dan kewajiban semua pihak dalam kegiatan pemrosesan informasi pribadi, mendorong penggunaan informasi pribadi yang wajar, melindungi perkembangan industri terkait, dan menyediakan peraturan yang komprehensif untuk pemroses informasi pribadi. Undang-undang ini menetapkan kewajiban perlindungan informasi pribadi khusus untuk platform Internet besar, seperti membangun sistem kepatuhan perlindungan informasi pribadi yang baik sesuai dengan peraturan nasional dan membentuk badan independen yang sebagian besar terdiri dari anggota eksternal untuk mengawasi

perlindungan informasi pribadi, mengikuti prinsip-prinsip keterbukaan, keadilan, dan ketidakberpihakan, merumuskan aturan platform, mengklarifikasi norma-norma penanganan informasi pribadi oleh penyedia produk atau layanan dalam platform, melindungi kewajiban informasi pribadi, berhenti memberikan layanan kepada penyedia produk atau layanan dalam platform yang secara serius melanggar hukum dan peraturan administratif dalam menangani informasi pribadi, dan secara teratur menerbitkan laporan tanggung jawab sosial tentang perlindungan informasi pribadi dan menerima pengawasan sosial. Ketentuan-ketentuan ini kondusif untuk meningkatkan transparansi operator platform Internet besar, meningkatkan tata kelola platform, memperkuat pengawasan eksternal, dan membentuk mekanisme perlindungan informasi pribadi dengan partisipasi seluruh masyarakat. Kedua, undang-undang industri dan lokal. Berbagai industri memiliki peraturan dan peraturan yang berbeda yang berkaitan dengan manajemen kepatuhan privasi data. Peraturan tentang Perlindungan Informasi Pribadi Pengguna Telekomunikasi dan Internet dikeluarkan pada bulan Juli 2013 oleh Kementerian Perindustrian dan Teknologi Informasi.

Peraturan ini menjelaskan bagaimana operator bisnis telekomunikasi dan penyedia layanan informasi Internet harus menjaga informasi pribadi pengguna aman. Selain itu, ada juga peraturan dan regulasi industri seperti Peraturan tentang Administrasi Keamanan Informasi Pribadi Pengguna Jasa Pengiriman Surat, Peraturan tentang Pelaporan dan Penanganan Informasi Keamanan di Industri Pos, Peraturan tentang Administrasi Bisnis Kartu Kredit, Langkah-langkah tentang Administrasi Identifikasi Pelanggan dan Penyimpanan Data Identifikasi Pelanggan dan Rekaman Transaksi Institusi Keuangan, dan Langkah-langkah Sementara tentang Administrasi Basis Data Dasar Informasi Kredit Pribadi. Ada juga beberapa dokumen normatif industri dan dokumen panduan, seperti Pemberitahuan Bank Rakyat Tiongkok tentang Perbankan Lembaga Keuangan untuk Melakukan Pekerjaan yang Baik dalam Melindungi Informasi Keuangan Pribadi, dan Panduan untuk Melindungi Informasi Pribadi dalam Teknologi Keamanan Informasi Sistem Informasi Layanan Publik dan Komersial. Selain itu, Panduan Perlindungan Informasi Pribadi dalam Teknologi Keamanan Informasi Sistem Informasi Layanan Publik dan Komersial, yang secara resmi diimplementasikan pada tanggal 1 Februari 2013, merupakan dokumen teknis panduan standar nasional pertama untuk perlindungan informasi pribadi di Tiongkok.

Peraturan tentang Manajemen Keamanan Data Besar di Kota Guiyang diadopsi pada pertemuan ke-13 Komite Tetap Kongres Rakyat ke-14 Kota Guiyang pada tanggal 5 Juni 2018 dan disetujui oleh pertemuan Komite Tetap Kongres Rakyat ke-13 Provinsi Guizhou pada tanggal 2 Agustus 2018. Ini adalah peraturan lokal pertama tentang manajemen keamanan data

besar di Tiongkok. Selain itu, setelah diputuskan pada pertemuan kedua mereka pada 29 Juni 2021, Komite Tetap Kongres Rakyat Shenzhen mengeluarkan Peraturan Data Zona Ekonomi Khusus Shenzhen pada 6 Juli 2021, yang berlaku mulai 1 Januari 2022. Sebagai peraturan daerah, peraturan ini untuk pertama kalinya mengedepankan hak-hak data individu, badan hukum, dan organisasi yang tidak berbadan hukum, termasuk data pribadi dan publik, elemen pasar data, keamanan data, dan topik lainnya.

BAB 6
Mengendalikan Risiko Transaksi dalam E-commerce

6.1 Identifikasi Risiko Transaksi Perdagangan Elektronik

Risiko transaksi e-commerce dapat dilihat dari berbagai sudut pandang, seperti tahap transaksi, konten transaksi, peserta transaksi, metode pembayaran, dan sebagainya. Dalam sudut pandang ini, risiko transaksi dapat dibagi menjadi risiko pra-transaksi, risiko dalam transaksi, dan risiko pasca-transaksi.

6.1.1 Risiko Pra-Transaksi Perdagangan Elektronik

1. Risiko Identitas

Operator platform e-commerce, konsumen, dan peserta e-commerce lainnya dapat menghadapi risiko identitas. Sebelum transaksi e-commerce dimulai, risiko identitas biasanya sudah ada dan sebagian besar disebabkan oleh perilaku yang disengaja. Penipuan transaksi dengan memalsukan identitas, misalnya Para pihak dalam transaksi salah memahami siapa pihak lain dalam transaksi, yang menghilangkan unsur para pihak dan membuat transaksi kehilangan efek hukumnya. Pada saat yang sama, ada juga risiko identitas yang disebabkan oleh kelalaian, serta risiko pengumpulan dan penggunaan informasi identitas konsumen oleh platform e-commerce dan operator platform. Risiko identitas membuat pihak lain, terutama konsumen, berisiko mengalami kerugian, yang pada akhirnya akan mengganggu operasi normal bisnis e-commerce. Risiko identitas meliputi kemungkinan identitas palsu, kemungkinan kerancuan identitas, dan kemungkinan pengumpulan dan penggunaan informasi identitas konsumen.

Pertama, risiko penyebaran informasi palsu. Semua pihak yang terlibat dalam bisnis e-commerce, khususnya operator dan pengguna platform, harus memberikan informasi identitas yang relevan secara jujur dan lengkap. Semua peserta memiliki konten berbeda dalam informasi identitas. Operator e-commerce terutama terdiri dari operator platform e-commerce; informasi identitas operator platform termasuk situs web operasi yang nyata dan efektif, izin usaha dari lembaga terdaftar, izin administratif yang terkait dengan bisnis mereka, atau tautan informasi. Informasi identitas operator platform termasuk nama terdaftar, kode kredit sosial terpadu, alamat bisnis yang sebenarnya, informasi kontak, nama toko, dan informasi lainnya. Informasi identitas pribadi pelanggan biasanya mencakup nama asli, nomor kontak, dan informasi lainnya.

Ada dua jenis kemungkinan operator e-commerce menggunakan identitas palsu. Yang pertama adalah platform e-commerce yang memenuhi syarat secara hukum dan operatornya

tidak memberikan informasi yang akurat atau sepenuhnya tidak akurat. Yang kedua adalah platform dan operator platform yang melakukan tindakan ilegal. Operator di platform paling rentan terhadap penipuan di antara peserta transaksi e-commerce, seperti yang ditunjukkan oleh masalah-masalah berikut: Pertama, operator platform menggunakan nama pengguna orang lain untuk melakukan bisnis tanpa izin. Beberapa platform e-commerce mungkin tidak memiliki registrasi badan utama pasar, tetapi menurut peraturan perundang-undangan mereka harus. Dalam industri seperti makanan, kosmetik, produk perawatan kesejahteraan, dan kosmetik, operator dapat menggunakan nama pengguna orang lain untuk melakukan bisnis tanpa izin. Beberapa platform perdagangan elektronik memiliki "iluminasi" atau toko online yang belum didaftarkan. Setelah itu, ujian kualifikasi dan pendaftaran operator di platform hanyalah formalitas. Beberapa izin usaha yang diunggah melalui sertifikasi toko online, nama operator yang sebenarnya, situs web perusahaan, bentuk komposisi, dan informasi lainnya jelas tidak sesuai dengan informasi izin usaha yang dipublikasikan. Beberapa bahkan mengunggah informasi izin usaha orang lain. Selain itu, sistem pengelolaan identitas pengguna tidak ketat. Beberapa operator platform e-commerce tidak memeriksa identitas pengguna dan nama toko operator dengan ketat, yang mengakibatkan penyesatan konsumen dan pelanggaran hak dan kepentingan yang sah seperti hak eksklusif untuk mendaftarkan merek dagang dan nama perusahaan.

Sistem anonim merupakan sumber utama risiko penyalahgunaan informasi identitas konsumen. Sebagai contoh, pinjaman berbahaya umumnya ditemukan di sektor keuangan P2P, menyebabkan perilaku pinjaman yang menyerupai kredit pengguna yang tidak diketahui atau identitas pinjaman yang sebenarnya, yang menyebabkan lebih banyak kredit macet.

Kedua, ada kemungkinan mengalami kebingungan identitas karena perilaku yang mengakibatkan kebingungan identitas. Kebingungan identitas mengacu pada penggunaan nama domain, nama, dan tanda secara ilegal dari situs web, departemen pemerintah, dan organisasi sosial lainnya. Ada dua jenis kebingungan identitas: yang pertama adalah penggunaan nama domain, nama, logo, atau situs web terkenal yang tidak sah yang membuat pelanggan terlihat seperti orang lain. Yang kedua adalah penggunaan yang tidak sah dari identitas elektronik palsu yang berasal dari departemen pemerintah atau organisasi sosial. Persaingan tidak sehat pada dasarnya menyebabkan kebingungan identitas.

Ketiga, ancaman pengumpulan dan penggunaan informasi identitas yang melanggar hukum. Ketika konsumen menggunakan layanan akses situs web atau menggunakan layanan rilis informasi yang disediakan oleh penyedia layanan jaringan, mereka harus memberikan informasi identitas yang benar kepada penyedia layanan jaringan. Namun, penyedia layanan

jaringan harus mematuhi undang-undang saat mengumpulkan dan menggunakan data pribadi warga negara. Dalam kasus di mana pelanggan melakukan transaksi dengan operator melalui platform e-commerce, informasi pribadi warga negara dapat dibagikan kepada operator dan penyedia layanan logistik yang terlibat dalam transaksi tersebut. Ini berbeda dengan informasi identitas operator yang dapat diakses oleh publik yang tidak ditentukan, dan informasi pelanggan hanya dapat diakses oleh entitas tertentu. Dalam kenyataannya, operator dan platform e-commerce seringkali tidak dapat menahan diri dari keinginan untuk menghasilkan keuntungan. Akibatnya, mereka mengumpulkan dan menggunakan informasi pribadi konsumen dengan cara yang melanggar hukum. Ini termasuk mengumpulkan, merusak, menghancurkan, menjual, atau memberikan secara ilegal kepada orang lain. Oleh karena itu, informasi pribadi konsumen dilindungi oleh hukum dan peraturan Tiongkok tentang pengumpulan dan penggunaan informasi identitas yang melanggar hukum.

2. Risiko Pemasaran

Terutama, risiko pemasaran mengacu pada kemungkinan menjual barang dan jasa secara ilegal. Jenis-jenis perilaku berikut ini termasuk dalam kategori ini.

Pertama, informasi yang tidak lengkap tentang komoditas atau layanan. Operator yang menyediakan barang atau jasa melalui jaringan, telepon, televisi, atau pesanan pos tidak memberikan informasi tentang kuantitas dan kualitas barang atau jasa, harga atau biaya, jangka waktu dan cara, tindakan pencegahan dan peringatan risiko, layanan purna jual, dan informasi tanggung jawab perdata kepada konsumen. Dalam mempromosikan barang atau jasa, penyelenggara e-commerce tidak memberikan informasi penting seperti nama, jenis, jumlah, kualitas, harga, metode pengiriman, distribusi, metode pembayaran, dan metode pengembalian dan penukaran.

Kedua, tindakan promosi palsu dan penipuan harga. Perilaku penipuan harga dan promosi palsu termasuk mengurangi harga asli yang tidak asli, menggunakan harga atau metode harga yang menyesatkan, menipu, membujuk pelanggan, mengurangi kualitas produk promosi (termasuk hadiah dan hadiah penjualan), menghalangi pertukaran, mempertahankan interpretasi akhir, dan merusak hak dan kepentingan konsumen. Beberapa operator dan platform e-commerce menawarkan perilaku konsumen yang jelas menyesatkan; beberapa operator platform menawarkan "harga sebelum aktivitas, diskon", "diskon rendah untuk menarik perhatian konsumen, setelah tidak ada inventaris", "kegagalan untuk mendorong konsumsi buta", dan "perubahan sepihak atau bahkan pembatalan program promosi." Penipuan harga baru yang dikenal sebagai "killing big data" telah muncul dalam beberapa tahun terakhir.

Ketiga, menjual barang virtual sebagai hadiah, dan jumlah barang virtual yang disepakati di pasar online melampaui batas yang ditetapkan dalam Undang-Undang Anti-Persaingan Usaha Tidak Sehat Republik Rakyat Tiongkok; atau nilai maksimum hadiah (kupon setara kas, kepemilikan fisik atau hak penggunaan, mata uang elektronik, dll.) melampaui batas yang ditetapkan dalam Undang-Undang.

Keempat, menyebarkan iklan yang tidak benar dan melanggar hukum, serta melakukan publisitas palsu. Dalam iklan, konten harus: tidak benar, ilegal, tidak jelas, dan sulit dipahami; menggunakan bahasa, teks, gambar, atau foto yang tidak benar dan menyesatkan; dan menggunakan berbagai publisitas palsu untuk menipu pelanggan. Operator platform tertentu mengiklankan produk mereka dengan menggunakan bahasa absolut seperti "harga terendah", "harga terendah dalam sejarah", dan "volume penjualan pertama", sementara operator platform lainnya menyebarkan iklan palsu yang menyesatkan dan tidak menjual barang atau jasa yang harus disetujui. Beberapa operator e-commerce dan konsumen memposting iklan palsu, informasi sensitif, dan "irigasi", serta sejumlah besar "komentar spam" di aplikasi sosial. Selain itu, beberapa operator lain memanfaatkan kerentanan API situs jejaring sosial untuk mempromosikan iklan di sana.

Kelima, pembuatan data transaksi palsu dan informasi bisnis palsu, termasuk brushing, brush ranking, dan kecurangan informasi, antara lain Salah satu jenis penipuan data bisnis adalah brushing. Pedagang di platform menciptakan ilusi bahwa mereka dapat menjual produk dengan stok terbatas. Memalsukan informasi bisnis dan menipu orang lain, termasuk konsumen, adalah cara operator berperilaku di platform pra-transaksi. Peringkat sikat adalah istilah yang mengacu pada berbagai metode yang dapat digunakan untuk mencapai tujuan pemeringkatan. Misalnya, gunakan akun nyata tanpa banyak catatan untuk menyikat penjualan produk tertentu di sebuah toko dan kemudian menggantinya dengan produk lain untuk membuat toko tersebut lebih disukai. Perilaku seperti ini lebih sering terjadi di platform e-commerce, game, dan mesin pencari, yang seringkali menyebabkan kerugian besar bagi pelanggan. Kecurangan informasi mengacu pada perilaku pedagang yang menghasilkan data transaksi palsu yang menghasilkan berbagai jenis data virtual, seperti penggemar, tampilan halaman, dan pemungutan suara, jika terjadi karena masalah sistem atau mesin otomatis lainnya.

Keenam, tindakan yang merugikan bisnis beberapa karyawan di dalam platform e-commerce diduga menerima suap bisnis, mencari peluang perdagangan yang menguntungkan secara tidak patut, dan menghalangi operator dari memasuki toko unggulan, peringkat pencarian, bilah iklan, dan halaman beranda lainnya.

Pelanggaran hak kekayaan intelektual atau produksi dan penjualan barang palsu dalam kegiatan promosi adalah contoh lain dari risiko pemasaran.

3. Risiko Aturan Perdagangan Platform

Aturan perdagangan platform adalah aturan yang dibuat, diubah, dan diterapkan oleh operator platform e-commerce untuk tujuan yang tidak spesifik dan berkaitan dengan kepentingan sosial dan publik yang berlaku untuk penggunaan layanan yang disediakan oleh platform.

Ada tiga jenis aturan perdagangan platform: aturan perdagangan platform pihak ketiga, aturan perdagangan platform yang dioperasikan sendiri, dan aturan perdagangan platform campuran. Aturan ini mengatur hubungan antara peserta platform, termasuk hubungan antara operator dan pengguna platform, dan hubungan antara operator dan pengguna platform secara internal. Karena aturan transaksi dibuat sebelum para pihak melakukan transaksi, lebih masuk akal untuk mengkategorikan risiko pelanggaran aturan transaksi sebagai risiko pra transaksi.

Operator e-commerce dan operator dalam platform adalah yang paling rentan terhadap aturan perdagangan platform. Karena operator dalam platform sering dipromosikan secara tidak akurat, mereka hanya dapat membuat, mengubah, dan mempublikasikan aturan perdagangan. Dengan membatasi jumlah operator platform dan ketentuan peraturan perdagangan yang diajukan ke otoritas pemerintah yang berwenang, risiko peraturan perdagangan platform sangat diminimalkan.

Terutama, aturan dasar, tanggung jawab dan pembagian risiko, perlindungan kekayaan intelektual, evaluasi kredit, perlindungan hak-hak konsumen, pengungkapan informasi, pencegahan dan penghentian informasi ilegal, penyelesaian sengketa perdagangan, aturan perdagangan, dan aturan perdagangan yang diperlukan lainnya menunjukkan risiko aturan perdagangan platform.

kegagalan untuk mematuhi prinsip-prinsip keterbukaan, kewajaran, dan keadilan, serta kegagalan untuk mematuhi hukum, undang-undang, dan etika sosial. sehingga mengganggu struktur ekonomi dan sosial. Mengganggu kepentingan masyarakat dan umum.\

6.1.2 Risiko dalam Transaksi E-commerce

Transaksi e-commerce terutama menghadapi risiko penandatanganan kontrak yang melanggar hukum, perilaku transaksi yang melanggar hukum, risiko pembayaran, dan risiko distribusi logistik.

1. Penandatanganan kontrak adalah illegal

Setiap tindakan yang dilakukan oleh peserta transaksi yang melanggar Hukum Perdata Republik Rakyat Tiongkok, Hukum Tanda Tangan Elektronik Republik Rakyat Tiongkok, dan ketentuan lainnya di Republik Rakyat Tiongkok disebut sebagai pelanggaran kontrak. Situasi-situasi berikut dapat terjadi.

Pertama, penerapan persyaratan konvensional yang tidak adil melanggar hak-hak konsumen. Ini terjadi dengan beberapa platform perdagangan jaringan dalam perjanjian layanan, pernyataan hukum, perjanjian layanan, aturan yang relevan, pernyataan hak cipta dan merek dagang, persyaratan layanan, pernyataan privasi, dll., yang diformat dalam kontrak untuk mengecualikan atau membatasi hak konsumen, mengurangi atau membebaskan operator dari tanggung jawab, meningkatkan tanggung jawab konsumen, atau semuanya.

Kedua, persyaratan yang tidak masuk akal yang dilampirkan selama proses penyediaan layanan platform bertentangan dengan keinginan pengguna. Beberapa operator platform e-commerce memanfaatkan dominasi mereka di pasar selama kegiatan promosi besar-besaran untuk memaksa pemasok yang berpartisipasi dalam promosi tersebut untuk meninggalkan platform e-commerce lain.

Ketiga, pihak yang bertransaksi tidak menggunakan tanda tangan elektronik sesuai dengan hukum. Jika masing-masing pihak dalam transaksi menandatangani kontrak dengan tanda tangan elektronik, mereka tidak mengikuti ketentuan hukum tentang tanda tangan elektronik dan menggunakan tanda tangan elektronik yang dapat diandalkan. Misalnya, jika tanda tangan elektronik membutuhkan otentikasi pihak ketiga, tanda tangan tersebut tidak memilih penyedia layanan otentikasi elektronik yang dapat diandalkan.

2. Perilaku transaksi illegal

Jenis utama perilaku perdagangan ilegal termasuk perilaku perdagangan yang tidak memenuhi syarat, perilaku ilegal dalam bentuk perdagangan atau target perdagangan, dan persaingan tidak sehat.

Pertama, perilaku perdagangan yang tidak memenuhi syarat. Perilaku perdagangan yang tidak memenuhi syarat termasuk menghindari hukum, peraturan, dan kebijakan yang memenuhi syarat, seperti berdagang sekuritas dan berjangka; menawarkan layanan untuk operator ilegal dan perdagangan ilegal; menjual barang khusus seperti bahan berbahaya dan beracun, obat-obatan, dan bahan kimia berbahaya; dan

Kedua, elemen yang berkaitan dengan bentuk transaksi atau tujuan transaksi dari perilaku ilegal. Tindakan ilegal dalam bentuk transaksi atau sasaran transaksi termasuk melakukan

transaksi yang dilarang oleh undang-undang dan peraturan, seperti perjudian, pencucian uang, skema piramida, dan penjualan perangkat lunak bajakan.

Ketiga, tindakan buruk yang dilakukan pesaing Perilaku tidak sehat, seperti intervensi tidak sengaja dalam evaluasi kredit, terjadi selama proses transaksi e-commerce. Operator di platform tertentu berusaha meningkatkan reputasi perusahaan mereka untuk diri mereka sendiri atau orang lain dengan melakukan transaksi palsu, menghapus ulasan negatif, atau merusak reputasi perusahaan pesaing dengan memberikan ulasan yang tidak masuk akal. Operator platform e-commerce tidak melakukan pengawasan dan pengendalian yang tepat. Akibatnya, beberapa karyawan internal bahkan terlibat dalam tindakan ilegal atau memberikan kemudahan dan kondisi yang tidak sesuai. Pada platform e-commerce, perilaku "menyikat inventaris" menyebabkan persaingan tidak sehat di antara pesaing, karena "menyikat inventaris" adalah perilaku transaksi palsu berskala besar yang hanya menandatangani pesanan tanpa pembayaran. Selain itu, "menyikat inventaris" termasuk dalam serangan pemerasan bisnis, di mana penyerang memasukkan sejumlah besar produk inventaris tetapi bukan perilaku pembayaran yang sebenarnya, sehingga pelanggan biasa tidak dapat membeli Serangan "inventaris menyikat" lebih sering terjadi pada pedagang baru yang mendorong pertumbuhan data melalui harga yang lebih rendah.

Konsumen tidak terlalu kuat, tetapi mereka juga dapat melakukan beberapa transaksi yang melanggar hukum untuk merusak hak dan kepentingan yang sah dari pihak yang terlibat dalam perdagangan. Konsumen lebih sering melakukan tiga transaksi jahat: kecurangan, penyalahgunaan wewenang, dan pembelian murah.

Kecurangan adalah perilaku konsumen yang menggunakan metode teknis untuk mengganggu transaksi normal, seperti mengambil barang untuk mendapatkan poin dan kemudian mengembalikannya kembali, yang pada dasarnya adalah transaksi palsu dan merugikan pedagang dan konsumen lain.

Di festival khusus, platform e-commerce sering mengeluarkan banyak voucher game, amplop merah, lalu lintas, kupon, dan aktivitas lainnya. Hacker dapat menipu dengan mengubah kode program. Misalnya, beberapa pedagang sering mengadakan ratusan kegiatan gratis pertama untuk meningkatkan penjualan; penyerang menggunakan skrip otomatis untuk "membunuh" barang, sehingga pedagang menjual sejumlah besar pengembalian berbahaya, pengembalian uang, sehingga konsumen biasa tidak dapat membeli barang yang mereka butuhkan.

Penggunaan celah logis untuk membuat pelanggan secara ilegal membeli hak untuk membeli atau memiliki barang offline atau mendapatkan atau mencuri barang dan jasa secara

gratis, misalnya melalui program spekulasi atau brute force crack bypass permission, dikenal sebagai bypass izin.

Membeli dengan harga murah adalah perilaku konsumen yang menggunakan celah sistem untuk membeli barang atau jasa berharga tinggi dengan harga murah secara ilegal. Misalnya, ada beberapa platform e-commerce yang memiliki masalah logika. ID yang berbeda untuk barang atau jasa berbeda memiliki harga yang berbeda, sehingga penjahat menggunakan ID yang hanya dapat membeli barang atau jasa dengan harga tinggi.

3. Membayar risiko

Pertama, layanan pembayaran seperti Alipay, Tenpay, dan layanan pihak ketiga lainnya tidak memenuhi syarat. Oleh karena itu, bahaya seperti itu tidak terlalu sering terjadi.

Kedua, risiko yang terkait dengan pembayaran elektronik. Pembayaran online umum mengacu pada pembayaran online sebelum pengiriman dan merupakan definisi sempit dari pembayaran online. Transaksi e-commerce seperti Taobao, Tmall, dan platform e-commerce lainnya sering menggunakan metode pembayaran online ini. Selain itu, pembayaran online, seperti jaminan setoran, berubah. Konsumen menanggung risiko kerusakan atau kehilangan barang jika terjadi risiko pembayaran online.

Ketiga, nasihat tentang risiko perdagangan online tidak memadai. Operator platform e-commerce tidak secara wajar meminta pengguna untuk memperhatikan risiko transaksi; lembaga pembayaran tidak meminta pembayar untuk mengkonfirmasi sebelum mengeksekusi pesanan.

Keempat, penipuan terhadap pembayaran pelanggan Selama fase konfirmasi pembayaran, pedagang tidak dapat memastikan apakah pemegang akun yang sebenarnya mengakui pembayaran tersebut. Misalnya, pembayaran mungkin berasal dari pembayaran yang dilakukan menggunakan kartu kredit yang dicuri. Penipuan menggunakan kartu kredit yang dicuri untuk menunjukkan bahwa ada pembelian yang sebenarnya, tetapi pemegang kartu kredit sebenarnya mengklaim bahwa pembelian tersebut tidak sah dan tidak mau membayar biaya pembelian. Bisnis akan mengalami kerugian karena transaksi sudah terjadi.

Kelima, perilaku tarik tunai. Ini termasuk tarik tunai voucher, kartu kredit, produk pembayaran kredit, dan lainnya. Salah satu yang paling populer di antara mereka adalah platform pembayaran pihak ketiga untuk cash-out kartu kredit. Konsep cash-out ini mengacu pada pembelian dua produk selama pembayaran, salah satunya dibayar dengan voucher, dan yang lainnya dibayar dengan kartu kredit, sehingga Anda dapat langsung bebas risiko mencairkan voucher.

Keenam, ada risiko menerima barang dengan uang tunai. Ini mengacu pada penerimaan barang dengan berbagai cara, seperti uang tunai atau pembayaran elektronik, dll. Biasanya, platform e-commerce yang dioperasikan sendiri mendukung metode pembayaran dengan uang tunai. Dengan demikian, operator yang bekerja untuk platform tersebut dapat menghadapi risiko gagal menerima barang oleh pelanggan atau distributor.

Tujuh adalah pembayaran IOU. Ini adalah penjualan kredit yang dilakukan oleh pedagang setelah pembayaran konsumen. Pedagang mengambil risiko untuk pengiriman pertama.

Delapan, standar bisnis dan teknis pembayaran elektronik tidak sehat. Risiko pembayaran ini mencakup pembayaran elektronik seperti pembayaran pihak ketiga, pembayaran seluler, dan standar bisnis dan teknis yang relevan yang belum diterbitkan.

Kesembilan, risiko yang terkait dengan sistem pembayaran elektronik. Sistem pembayaran elektronik terdiri dari beberapa sistem: sistem jaringan informasi, sistem penyelesaian, sistem sertifikasi, sistem kredit, dan lembaga keuangan. Sistem jaringan informasi menyediakan layanan pembayaran elektronik, sedangkan sistem penyelesaian, sistem sertifikasi, sistem kredit, dan lembaga keuangan bertanggung jawab untuk mendukung layanan pembayaran elektronik. Setiap elemen sistem pembayaran elektronik akan menghadapi bahaya internal dan luar. Tentu saja, orang-orang yang menggunakan sistem pembayaran online, seperti pelanggan dan pedagang, juga harus menanggung risiko tertentu terkait keamanan pembayaran. Konsumen mudah terjebak ke situs web yang tidak dikenal, membocorkan informasi penting, atau mengalami penipuan jika mereka tidak memilih platform pembayaran dengan benar, tidak terampil dalam operasi pembayaran, dan tidak yakin dengan keamanan sistem mereka.

4. Risiko logistik dan distribusi

Logistik dan distribusi menghadapi beberapa masalah fundamental. Pilihan distributor logistik adalah yang pertama. Distributor biasanya menyarankan platform e-commerce. Kedua, logistik distribusi, yang mencakup pengiriman dari pintu ke pintu pedagang dan penjemputan dari pintu ke pintu pembeli. Ketiga, biaya dan distribusi logistik, yang mencakup pembayaran atau distribusi gratis (gratis bersyarat). Keempat, waktu distribusi logistik, yang mencakup komitmen (seperti "Jingdong da" JD, dengan waktu pengiriman yang akurat), dan tidak ada komitmen (seperti waktu pengiriman Tmall dan Taobao). Kelima, informasi distribusi dan logistik. Termasuk memberikan informasi tentang pengiriman, tetapi tidak tentang distribusi. Salah satu cara penting bagi penyedia logistik untuk meningkatkan layanan mereka adalah dengan memberikan informasi distribusi.

Salah satu risiko yang terkait dengan distribusi logistik adalah berikut: barang yang dikirim oleh logistik tidak sesuai dengan barang yang dibeli, yaitu barang yang dikirim tidak sesuai

dengan kategori, jumlah, atau kualitas barang yang dibeli; barang yang dikirim rusak atau hilang, yaitu barang yang dikirim rusak atau hilang selama transportasi dan distribusi, bahkan jika barang tersebut memiliki asuransi. Distributor logistik gagal bernegosiasi secara aktif dengan pelanggan dalam situasi yang buruk; misalnya, mereka dapat menyembunyikan informasi distribusi logistik.

6.1.3 Risiko Pasca-Transaksi Perdagangan Elektronik

1. Risiko bukti transaksi

Bukti transaksi adalah barang yang dapat menunjukkan bahwa ada transaksi yang benar, seperti data elektronik, materi, bukti dokumenter, bukti material, dll. Bukti transaksi e-commerce biasanya berupa data elektronik, seperti halaman kontrak, faktur elektronik, email, dll. Risiko bukti transaksi termasuk ketidakcocokan atau kurangnya bukti transaksi itu sendiri.

2. Risiko layanan purna jual

Pelanggaran hukum dan peraturan tentang layanan purna jual, atau pelanggaran komitmen purna jual khusus, menimbulkan risiko layanan purna jual. Pelanggaran hukum tentang layanan purna jual terutama mencakup operator e-commerce yang melanggar hukum dan peraturan tentang tujuh hari tanpa alasan untuk mengembalikan barang dan pelanggaran hukum tentang "tiga jaminan" (perbaikan, penggantian, dan pengembalian). Jika mereka gagal memenuhi janji mereka sesuai dengan perjanjian, misalnya, jika operator platform atau platform perdagangan pihak ketiga gagal memberikan layanan "margin penjual" kepada pelanggan, kontrak akan dilanggar.

3. Risiko penanganan sengketa transaksi

Penanganan sengketa transaksi yang tidak efektif oleh penyelenggara platform dan penyelenggara platform sendiri akan meningkatkan risiko penanganan sengketa transaksi. Penanganan sengketa transaksi yang buruk terutama ditunjukkan oleh para penyelenggara platform dalam menangani keluhan konsumen, tidak bersikap positif, dan bahkan bersikap buruk terhadap konsumen. Operator platform menangani sengketa transaksi yang buruk terutama mencakup hal-hal berikut: Operator platform tidak melakukan layanan pengembalian dan penukaran seperti yang dijanjikan atau hasil pengembalian dan penukaran tidak memuaskan pelanggan. Pertama, penipuan bisnis. Beberapa operator platform e-commerce gagal mengawasi dan menangani dugaan penipuan kontrak dan penipuan konsumen. Kedua, aturan manajemen internal yang tidak masuk akal. Beberapa operator platform e-commerce berurusan dengan perilaku kesibukan yang melanggar hukum dan peraturan nasional. Ini membuat operator ilegal atau calon operator ilegal berpikir biaya ilegal tidak tinggi dan

mendorong ekspektasi psikologis dan aktual mereka tentang perilaku mencari kepentingan yang tidak benar. Ketiga, konsumen belum dilindungi hak-haknya oleh penyelenggara platform e-commerce.

4. Mengevaluasi risiko

Terdapat dua jenis risiko evaluasi: risiko evaluasi berbahaya setelah penjualan dan risiko keluhan berbahaya setelah penjualan. Risiko evaluasi berbahaya setelah penjualan mengacu pada evaluasi yang dilakukan konsumen terhadap operator dalam platform melalui mekanisme evaluasi yang disediakan oleh platform e-commerce; keluhan meliputi keluhan dalam platform dan keluhan di luar platform. Konsumen dapat melakukan pengaduan yang tidak menyenangkan kepada operator platform e-commerce, dan mereka juga memiliki kemampuan untuk melakukan pengaduan yang tidak menyenangkan terhadap mereka.

6.2 Penilaian Risiko dan Pengambilan Keputusan Transaksi E-commerce

6.2.1 Sudut Pandang Asuransi Penilaian Risiko Transaksi E-commerce

Risiko transaksi e-commerce dapat dinilai dari berbagai sudut pandang. Pertama dan terpenting, evaluasi didasarkan pada tahap transaksi e-commerce. Ketika mengevaluasi risiko transaksi e-commerce, hal ini terutama bergantung pada tahap transaksi mana yang terjadi. Sebelum transaksi e-commerce, selama transaksi, dan setelah transaksi, akan ada risiko; jenis, karakteristik, dan frekuensi risiko berbeda.

Kedua, berdasarkan subjek evaluasi transaksi e-commerce. Dalam melakukan evaluasi berdasarkan subjek transaksi e-commerce, hal ini terutama bergantung pada pihak mana yang melaksanakan transaksi e-commerce. Meskipun operator platform jelas merupakan pihak yang paling berisiko dalam transaksi, konsumen dan operator platform e-commerce juga dapat menghadapi risiko. Ketiga, evaluasi didasarkan pada risiko yang terkait dengan transaksi e-commerce. Setelah risiko transaksi e-commerce, ada tiga konsekuensi: pelanggaran kontrak, ilegal, dan kriminal. Keempat, berdasarkan cara penilaian risiko transaksi e-commerce dilakukan. Risiko transaksi e-commerce dapat dibagi menjadi kategori normatif dan teknis berdasarkan jenisnya. Sebagian besar risiko yang terkait dengan transaksi e-commerce memiliki salah satu dari dua karakteristik di atas. Kelima, evaluasi mengacu pada faktor-faktor yang mempengaruhi risiko transaksi e-commerce dan bobotnya. Faktor-faktor ini terutama termasuk faktor teknis, faktor pasar, faktor hukum dan kelembagaan, faktor kredit, faktor pribadi, dll. Di antara faktor-faktor ini, faktor teknis terutama mengacu pada teknologi keamanan yang mempengaruhi transaksi e-commerce. Keamanan sistem perdagangan e-commerce akan dipengaruhi secara langsung oleh cacat, celah, atau pengoperasian atau

pemeliharaan yang tidak tepat dari teknologi keamanan. Faktor pasar terutama mengacu pada kondisi pasar di mana transaksi e-commerce dilakukan, terutama termasuk status kredit pasar, struktur informasi pasar, tingkat pengembangan, tingkat kesempurnaan, dll. Faktor manajemen juga mengacu pada faktor hukum dan kelembagaan, yang menunjukkan seberapa baik sistem pasar virtual berfungsi, seberapa baik transaksi e-commerce diawasi, dan seberapa baik peraturan dan hukum yang relevan diterapkan. Faktor kredit terutama mengacu pada faktor kredit yang terkait dengan transaksi e-commerce, termasuk sistem kredit dan kredit peserta dalam transaksi e-commerce, dll. Faktor pribadi adalah beberapa faktor yang terkait dengan karakteristik pribadi konsumen, terutama mencakup sikap pribadi konsumen terhadap risiko, kesadaran akan keselamatan, perilaku buruk, dll. Faktor-faktor ini berdampak pada risiko transaksi e-commerce secara berbeda, sehingga beratnya juga berbeda.

6.2.2 Sistem Indeks Evaluasi Risiko Transaksi E-commerce

Karena operator e-commerce adalah peserta utama dalam transaksi e-commerce, indikator evaluasi risiko transaksi untuk operator platform e-commerce dan operator dalam platform akan dibahas secara khusus di sini.

1. Indeks evaluasi risiko transaksi operator platform e-commerce

Untuk menilai risiko transaksi dari operator platform e-commerce, ada beberapa indikator. Yang pertama adalah indeks kualifikasi platform e-commerce, yang mencakup indikator modal terdaftar, profesional, kemampuan layanan, dan langkah-langkah keamanan platform e-commerce. Kedua, indikator manajemen operator platform. Indikator ini mencakup mekanisme audit operator dalam platform dan kualifikasi operator. Ketiga indikator audit komoditas adalah publisitas dan audit informasi komoditas, harga dan kualitas, serta indikator lainnya. Keempat, indeks proses layanan transaksi. Ini mencakup aturan perdagangan, pengelolaan kredit, penanganan sengketa, dan indikator lainnya. Kelima, indeks layanan pendukung. Indikator ini mencakup layanan logistik, layanan pembayaran elektronik, dan indikator lainnya. Keenam, indikator keamanan dan kerahasiaan informasi. Indikator ini termasuk indikator keamanan informasi, indikator teknis, dan lainnya.

2. Indikator evaluasi risiko transaksi dari operator dalam platform

Indikator yang digunakan operator untuk menilai risiko transaksi di platform ini mencakup elemen-elemen berikut. Ada dua indeks status bisnis. Yang pertama adalah indeks legalitas bisnis, yang menunjukkan kualifikasi bisnis legal, konten bisnis legal, perilaku bisnis legal, dan sebagainya. Yang kedua adalah indeks status bisnis, yang menunjukkan waktu bisnis, volume perdagangan, status keuangan, sumber daya manusia, dan indikator lainnya.

Ketiga, indikator pengungkapan informasi dan manajemen. Indikator ini termasuk informasi tentang produk, harga, biaya, dan deskripsi layanan, informasi tentang aktivitas, aturan platform dan manajemen privasi, status kredit, dan indikator lainnya. Keempat, indikator kualitas produk atau layanan. Ini mencakup faktor-faktor seperti kualitas produk atau layanan yang dijelaskan oleh operator serta tingkat yang diharapkan oleh konsumen. Kelima, indikator layanan pembayaran dan distribusi. Indikator ini mencakup keamanan pembayaran, fungsionalitas, kenyamanan, serta keamanan pengiriman, ketepatan waktu, biaya layanan, dan elemen lainnya. Keenam, indikator dan keluhan layanan pelanggan.

Indikator kepuasan pelanggan dan keluhan: kepuasan pelanggan mencakup kualitas barang atau jasa, kualitas layanan logistik, pengalaman berbelanja, dll. Keluhan mencakup jenis keluhan, jumlah, proporsi, dll.

6.2.3 Keputusan Pengendalian Risiko Transaksi E-commerce

Pemerintah dan perusahaan bertanggung jawab atas pengendalian risiko transaksi e-commerce. Operator platform berbeda dari operator e-commerce lainnya karena mereka memiliki kemampuan untuk mengatur kelompok bilateral atau multilateral untuk melakukan transaksi. Ini memiliki dampak jaringan yang kuat, terutama jaringan lintas batas, yang berdampak besar pada alokasi sumber daya dan memberikan status ganda sebagai penyelenggara dan pelaku pasar. Misalnya, Taobao mengawasi perdagangan, menjaga persaingan, dan membuat sistem kredit. Dalam platform e-commerce, pelanggaran, pemalsuan, publisitas palsu, dan promosi palsu telah meningkat dalam beberapa tahun terakhir. Data yang dirilis oleh otoritas pengawas China pada tahun 2017 menunjukkan bahwa, meskipun proporsi pengaduan barang palsu dan barang e-commerce yang tidak memenuhi syarat semuanya menurun, proporsi total pengaduan pelanggaran paten di e-commerce meningkat secara signifikan.

Kontrol kooperatif dari berbagai aspek telah menjadi keharusan untuk pengendalian risiko transaksi e-commerce karena perusahaan e-commerce terus berkembang dan struktur ganda "pemerintah dan perusahaan" tradisional menjadi kurang efektif.

1. Mode kontrol kolaboratif dari partisipasi bersama oleh beberapa subjek

Metode kontrol kooperatif di mana berbagai subjek bekerja sama untuk menyelesaikan kontrol risiko transaksi e-commerce dengan memberikan peran penuh kepada pemerintah, organisasi industri, perusahaan e-commerce, dan lembaga publik. Organisasi pengatur internal perusahaan e-commerce membuat sistem dan prosedur yang tepat untuk membuat operasi mereka legal dan patuh dan untuk mengendalikan risiko transaksi dengan baik. Etika

profesional ditetapkan sebagai dasar organisasi, anggotanya dikelola melalui disiplin diri dan aturan perdagangan, dan membentuk sistem inspeksi diri dan timbal balik, yang juga memainkan peran penting dalam pengawasan pemerintah. Dalam hal biaya, batas waktu, dan teknologi pengendalian risiko, perusahaan perdagangan elektronik memiliki lebih banyak keuntungan daripada pengawasan pemerintah. Pengawasan publik dapat memaksa pemerintah untuk memperkuat regulasi dan menciptakan pasar yang adil, tertib, dan sehat.

2. Kolaborasi antara pemerintah dan platform e-commerce

Pemerintah dan perusahaan e-commerce—terutama platform e-commerce—harus bekerja sama untuk mengontrol berbagai masalah secara kolaboratif, dan masalah-masalah berikut harus diselesaikan. Pertama, membagi tanggung jawab yang wajar antara pemerintah dan perusahaan e-commerce melalui mode tata kelola kolaboratif. Ini akan mencegah pemerintah memberikan tanggung jawab yang berlebihan kepada perusahaan e-commerce dan mempertahankan vitalitas inovasi dan pengembangan mereka. Kedua, pemerintah harus membuat sistem hukum yang sesuai dengan karakteristik perusahaan lembah elektronik. Sistem pengawasan pemerintah harus menurunkan biaya, meningkatkan efisiensi kontrol kolaboratif, mendorong pelaksanaan tanggung jawab perusahaan perdagangan elektronik, dan meningkatkan efisiensi regulasi. Tingkat keterlibatan pemerintah dan perusahaan e-commerce dalam pengendalian risiko harus berbeda-beda di bidang yang berbeda.

6.3 Implementasi Pengendalian Risiko Transaksi E-commerce

6.3.1 Konsep dan Properti Spesifikasi

Dimungkinkan untuk membagi pengendalian risiko transaksi e-commerce menjadi dua kategori: pengendalian risiko teknis. Bab 4 "Mengendalikan Risiko Informasi dalam Perdagangan Elektronik" dan Bab 5 "Mengendalikan Risiko Jaringan dalam Perdagangan Elektronik" membahas langkah-langkah pengendalian risiko teknis. Namun, pengendalian risiko normatif terutama dibahas di sini. Untuk mengendalikan risiko normatif transaksi e-commerce, pemerintah, organisasi industri, komunitas, dan individu lain yang terlibat dalam pengendalian transaksi e-commerce dapat membuat standar yang sesuai. Selanjutnya, sesuai dengan hak dan tanggung jawab mereka, subjek kontrol ini akan mengambil tindakan pengendalian risiko khusus.

1. Konsep spesifikasi yang relevan

Dalam norma, "peraturan" berarti penguasa, "kipas" berarti cetakan, dan "peraturan" awalnya berarti pengekangan material atau material, dan perluasannya berarti kekuatan yang mengontrol pemikiran dan perilaku seseorang. Hukum, standar, peraturan industri, etika,

kebijakan, dan peraturan perusahaan adalah semua contoh standar. Perlu dicatat bahwa doktrin, teori, dan model matematis juga memiliki sifat normatif; namun, komentar tidak dibuat di sini karena tidak berkaitan dengan pengendalian risiko.

Pertama, hukum. Konstitusi dan undang-undang Tiongkok, peraturan administratif, dokumen dan aturan normatif, peraturan lokal, perjanjian internasional, interpretasi yudisial, dll. adalah contoh formalisme hukum Tiongkok. Untuk konsep yang relevan, lihat Bagian 4.3.

Kedua, norma. Menurut Bagian 1: Terminologi Umum untuk Standardisasi dan Kegiatan Terkait (GB/T 20000.1-2014), "standar" adalah dokumen yang menyediakan aturan, pedoman, atau fitur untuk penggunaan dan penggunaan ulang secara umum, melalui kegiatan yang terstandardisasi, sesuai dengan prosedur yang ditentukan. Tiga standar utama yang berkaitan dengan perdagangan e-commerce adalah Model E-commerce Specification (GB/T 36310-2018), Spesifikasi Layanan Belanja Online (SB/T 1059-2009), dan Spesifikasi Layanan Platform Perdagangan E-commerce Pihak Ketiga (Announcement COM No. 18, 2011).

Ketiga, peraturan bisnis. Organisasi industri adalah kelompok sosial nirlaba sipil yang dibentuk oleh anggota industri untuk kepentingan bersama. Konvensi industri, juga disebut konvensi disiplin diri industri, konvensi manajemen diri industri, atau akta publik, mengatur organisasi industri untuk menjaga perkembangan industri yang berkelanjutan dan sehat untuk semua anggota kode yang mengikat secara universal. Organisasi industri juga dikenal sebagai manajemen disiplasi industri. Konvensi industri membantu organisasi industri mengendalikan dan mengatur diri mereka di luar pengawasan pemerintah dan sosial.

Keempat, peraturan yang berkaitan dengan perusahaan. Peraturan dan regulasi perusahaan adalah peraturan dan peraturan yang digunakan oleh perusahaan untuk mengatur semua pekerjanya dan semua kegiatan ekonominya. Ini adalah implementasi dari sistem tanggung jawab ekonomi internal organisasi. Perusahaan memiliki sistem dasar, sistem kerja, dan sistem tanggung jawab, dan setiap karyawan atau departemen harus mematuhi aturan dan peraturannya. Peraturan dan regulasi perusahaan harus didasarkan pada Undang-Undang Ketenagakerjaan Republik Rakyat Tiongkok dan tidak melanggar hukum. Peraturan dan regulasi perusahaan harus mencerminkan karakteristik dan persyaratan kegiatan ekonomi perusahaan.

Kelima, perjanjian dan aturan perdagangan. Aturan transaksi mengacu pada aturan dan perjanjian yang disepakati oleh semua pihak yang terlibat dalam proses transaksi e-commerce yang dibuat oleh operator e-commerce. Aturan ini terutama berkaitan dengan aturan perdagangan dan perjanjian layanan yang dibuat oleh operator platform e-commerce, dan kedua belah pihak berpartisipasi dalam proses perumusan aturan. Di antara mereka,

perjanjian adalah dokumen yang disebut sebagai "kontrak" yang biasa digunakan oleh kelompok sosial atau individu untuk menangani berbagai hubungan dan urusan sosial. Beberapa contoh dokumen "kontrak" termasuk, tetapi tidak terbatas pada, perjanjian, protokol, perjanjian, konvensi, deklarasi bersama, pernyataan bersama, dll.

Tabel 6.1 Objek dan tanggung jawab dari spesifikasi tanggung jawab

Proyek	Hukum	Standar Wajib	Konvensi Industri	Regulasi dan Aturan Perusahaan	Perjanjian Perdagangan
Objek yang Cocok	Semua Tubuh Utama	Semua Tubuh Utama	Anggota Industri	Karyawan Perusahaan	Peserta Transaksi
Siat Tanggung Jawab	Hukum Tanggung Jawab	Hukum Tanggung Jawab	Konvensi Tanggung Jawab	Aturan dan Tanggung Jawab	Tanggung Jawab atas Pelanggaran Kontrak

Tabel 6.2 Objek dan tanggung jawab yang berlaku dari spesifikasi panduan

Proyek	Standar yang Direkomendasikan	Moral	Kebijakan
Objek yang Cocok	Semua Tubuh Utama	Semua Tubuh Utama	Semua Tubuh Utama
Sifat Tanggung Jawab	Tidak ada tanggung jawab hukum	Tidak ada tanggung jawab hukum	Tidak ada tanggung jawab hukum

Keenam, etika. Moralitas mengacu pada prinsip-prinsip dan standar yang harus diikuti seseorang dalam berperilaku. Moralitas tidak dapat dibatasi oleh sanksi tertentu, tetapi hanya oleh hati nurani dan kebiasaan masyarakat. Oleh karena itu, hukum tidak memiliki kekuatan moral.

Ketujuh, peraturan. Prinsip-prinsip umum yang digunakan untuk mengarahkan pemerintah dalam menangani urusan publik dan badan legislatif dalam membuat undang-undang disebut kebijakan. Jika suatu perilaku melanggar etika atau memiliki kecenderungan yang berbahaya yang merusak kepentingan negara dan masyarakat, hukum menolak untuk mengakui dampak dari perilaku tersebut. Kebijakan publik dianggap bertentangan dengan tindakan ini.

2. Sifat spesifikasi

Sifat spesifikasi menentukan apakah spesifikasi tersebut memiliki kekuatan hukum untuk memaksakan sesuatu. Norma dengan paksaan hukum adalah norma wajib, seperti undang-undang, peraturan, konvensi industri, peraturan dan perjanjian transaksi, dll.; norma tanpa paksaan hukum adalah norma rekomendasi, seperti etika, kebijakan, dan standar. Pelanggaran

norma yang berbeda memiliki konsekuensi yang berbeda. **Tabel 6.1** menunjukkan objek yang berlaku dan karakteristik tanggung jawab dari standar wajib dan panduan.

6.3.2 Kepatuhan Transaksi Peserta dalam Transaksi E-commerce

Operator platform e-commerce, pedagang dalam platform, dan pelanggan biasanya terlibat dalam transaksi e-commerce. Ada tiga jenis pengendalian risiko partisipan transaksi e-commerce: pengendalian risiko platform e-commerce, pengendalian risiko operator platform, dan pengendalian risiko konsumen. Di atas pengendalian risiko juga mencakup pengendalian risiko dan pengendalian diri risiko pihak lain, khuxsusnya kewajiban pemeriksaan, verifikasi, inspeksi, dan monitor yang dilakukan oleh operator platform e-commerce. Pengumuman dari Dewan Negara tentang Percetakan dan Distribusi Rencana Pengawasan Pasar Lima Tahun ke-13 (No. 6, 2017) menyatakan bahwa praktik manajemen kontemporer harus dipatuhi untuk mengembangkan sistem tata kelola sosial baru yang menggabungkan konsep "otonomi perusahaan, disiplin pengawasan industri, pengawasan sosial, dan pengawasan pemerintah. Untuk meningkatkan Produsen dan operator memiliki tanggung jawab utama, dan perusahaan harus memenuhi tanggung jawab tersebut. mereka menangani layanan purna jual, manajemen kualitas, dan pemasaran dan publisitas. keamanan produksi, membangun perusahaan sebagai pengawas dan mempertahankan struktur industri dan lingkungan pasar, dan mengembangkan subjek pasar dengan kewajiban sosial. Kami akan memimpin organisasi ekonomi non-pemerintah. untuk mendukung pengembangan Partai dan liga pemuda, dan dengan cermat bertindak sesuai dengan peraturan dan hukum.

Risiko transaksi e-commerce dikontrol sebagian besar oleh peserta transaksi e-commerce. handel. Pertama dan terpenting, operator e-commerce harus membuat dan meningkatkan semua jenis aturan keamanan. Regulasi dan peraturan keselamatan undang-undang, peraturan, standar, kebijakan, dan peraturan terutama keselamatan nasional sesuai dengan persyaratan industri tertentu. Kedua, pihak yang melakukan transaksi e Bisnis harus mematuhi transaksi, khususnya dalam hal mengendalikan risiko pada tiga proses sebelum transaksi, selama transaksi, dan setelah transaksi.

1. Pengendalian risiko sebelum transaksi e-commerce

Pertama, individu yang berpartisipasi dalam transaksi e-commerce harus memenuhi persyaratan legal. Syarat Hukum yang berlaku untuk peserta transaksi e-commerce mencakup persyaratan hukum platform e-commerce dan operator platform tersebut, serta persyaratan hukum konsumen.

Operator dan platform e-commerce memenuhi persyaratan legal. Pertama, Pasal 8 dari Langkah-langkah dalam Manajemen Transaksi Online (dikeluarkan pada tanggal 15 Maret oleh Administrasi Negara untuk Peraturan Pasar 2021) melarang operator transaksi online untuk beroperasi tanpa izin yang melanggar undang-undang, peraturan, dan keputusan yang dibuat oleh Dewan Negara. Selain situasi tanpa persyaratan Undang-Undang Perdagangan Elektronik, operator Perdagangan online harus berurusan dengan entitas pasar yang diregistrasi sesuai dengan hukum. Individu yang melakukan perdagangan online, dan jumlah transaksi Tidak perlu mendaftar jika pendapatannya tahunan tidak melebihi 100.000 yuan. dengan persyaratan yang tercantum dalam Undang-Undang Perdagangan Elektronik. Kemudian, Menurut Pasal 10 Undang-Undang Perdagangan Elektronik, operator Perdagangan elektronik perlu menangani pendaftaran subjek pasar sesuai dengan hukuman Namun, orang-orang yang menjual produk pertanian dan produk sampingan industri rumahan, orang-orang yang terlibat dengan keterampilan mereka sendiri dalam kegiatan layanan tenaga kerja yang nyaman dan transaksi kecil yang kadang-kadang terjadi tidak perlu mendaftar sesuai atau mendapatkan izin sesuai dengan hukum dengan peraturan pemerintah dan hukum. Spesifikasi layanan yang terkait dengan Platform Menurut e-commerce pihak ketiga, operator platform harusmengawasi pendaftaran bisnis dan industri sesuai dengan hukum; jika lisensi administratif harus mendapatkan izin administratif dari departemen yang berkuasa. Operator peron harus mengajukan permohonan kepada operator peron untuk menyerahkan dokumen identifikasi atau izin usaha atau dokumen sertifikasi bisnis yang disetujui, informasi kontak dan alamat bisnis, dan informasi tambahan yang dibutuhkan. Operator platform harus memastikan izin bisnis, sertifikat pendaftaran pajak, serta berbagai izin usaha operator stasiun yang berbeda yang tersedia di platform, secara teratur memverifikasi daftar operator stasiun yang terdaftar setiap tahun dengan nama asli mereka, dan menunjukkan operator stasiun yang tidak dapat dipastikan. Pasal 27 Undang-Undang Perdagangan Elektronik mengatur bahwa operator platform perdagangan elektronik harus memaksa operator yang membuat permohonan untuk bergabung dengan platform untuk menjual barang atau menyediakan layanan yang memungkinkan penyerahan data akurat seperti identitas, melakukan verifikasi, mengumpulkan informasi seperti alamat, informasi kontak, izin administratif, dan sebagainya, registrasi, membuat file registrasi, dan memeriksa dan memperbarui file secara berkala. Operator platform perdagangan elektronik harus mengikuti peraturan yang berlaku dari bagian ini saat memberikan layanan kepada pengguna non-operator yang memasuki platform untuk menyediakan layanan atau menjual barang. Pasal 28 undang-undang perdagangan elektronik, operator platform e-commerce harus memenuhi persyaratan yang ditetapkan dalam kewajiban untuk departemen

pengawasan dan administrasi pasar menyerahkan informasi identitas operator platform, meminta operator untuk tidak berurusan pendaftaran badan utama pasar sesuai dengan pendaftaran, dan kolaborasi dengan departemen pasar dan pengawasan, sesuai dengan fitur e bisnis, untuk mengendalikan operator pendaftaran badan utama pasar yang menyediakan memahami. Operator platform e-commerce harus mematuhi peraturan hukum.peraturan administratif dan undang-undang pemungutan pajak, memberikan ke otoritas pajak melalui platform informasi pajak dan identitas, dan harus segera mematuhi ketentuan yang tercantum dalam Pasal 10 undang-undang ini dan tidak perlu pendaftaran subjek pasar operator e-commerce sesuai dengan ketentuan yang disebutkan di paragraf kedua Artikel 11 tentang pendaftaran pajak Undang-Undang Perdagangan Elektronik, Pasal 12 menetapkan bahwa operator perdagangan elektronik yang membutuhkan lisensi Ketika terlibat dalam kegiatan bisnis, administrator yang relevan harus mendapatkan izin administratif mengikuti peraturan.

Kriteria pelanggan adalah legal. Konsumen jaringan harus individu dengan kapasitas sipil tertentu.

Kedua, sesuai dengan hukum untuk mengungkapkan informasi identitas yang sebenarnya. Panjang pengungkapan informasi identitas bervariasi tergantung pada peserta. transaksi e-commerce, tetapi tidak masalah, pengungkapan data identitas Jenis peserta transaksi e-commerce, data identitas yang harus publikasi harus benar, tidak salah, atau membingungkan yang tidak dibutuhkan.

Informasi identifikasi operator platform harus dipublikasikan. Namun, untuk operator Pasal 12 dari Langkah-langkah Pengawasan dan Administrasi untuk Platform Perdagangan Online menyatakan bahwa operator harus terus mempublikasikan informasi yang berkaitan dengan subjek operator atau tautan ke informasi tersebut di tempat yang menonjol di halaman beranda atau halaman utama situs web mereka terlibat dalam aktivitas perusahaan. Operator perdagangan online disarankan untuk membangun hubungan ke sistem penerangan izin usaha elektronik Administrasi Negara untuk Regulasi Informasi perizinan perusahaan mereka dijual dan dipublikasikan. Menurut Pasal 15 UU Perdagangan Elektronik, operator Informasi izin usaha harus terus dipublikasikan oleh e-commerce pada posisi yang diutamakan di halaman web mereka, informasi izin administratif yang terkait dengan perusahaan mereka, pendaftaran subjek pasar sesuai dengan Pasal 10 UU ini, atau tautan ke logo dari informasi yang disebutkan di atas. Jika informasi yang disebutkan di atas berubah, operator e-commerce harus memberi tahu masyarakat segera. Aturan 16 Undang-Undang Perdagangan Elektronik mewajibkan operator perdagangan elektronik elektronik harus berhenti berpartisipasi dalam perdagangan elektronik. publikasikan informasi yang relevan di bagian depan halaman beranda 30 hari yang

lalu. Artikel 17 UU PMSE menetapkan bahwa penyelenggara Informasi komoditas atau layanan harus diungkapkan oleh PMSE. melindungi hak konsumen untuk mengetahui dan pilih. Penyelenggara e-commerce tidak boleh melakukan promosi yang menyesatkan atau menipu melalui transaksi fiktif atau memalsukan ulasan pengguna, atau menipu atau menipu pelanggan. Dalam hal publikasi informasi, standar Operator platform dan operator tidak sama. penyedia platform harus sepenuhnya memberikan informasi identitas platform. Situs: situs web atau platform harus menyampaikan data alamat IP secara elektronik sesuai dengan syarat memasukkan alamat IP dan mengungkapkan informasi catatan di di bawah halaman beranda dari situs web tersebut. Bisnis izin, sertifikat pendaftaran pajak, izin bisnis khusus (misalnya karena melibatkan bisnis khusus), alamat perusahaan nyata, Informasi seperti nomor telepon kontak dan informasi lainnya juga harus diungkapkan di bawah ini. halaman beranda dari situs web tersebut.

Mengumumkan identitas operator di platform. Mengenai lingkup informasi identitas operator dipublikasikan di platform, Spesifikasi Layanan untuk Menurut formulir perdagangan e-commerce pihak ketiga, apakah platform Nama asli dan nama operator ditunjukkan dalam perdagangan e-commerce pihak ketiga di Dengan bekerja sama, operator platform dan operator stasiun menentukan lokasi stasiun. Dengan kata lain, spektrum publikasi informasi identitas operator di platform dapat besar atau sederhana. Tetapi ketika sebuah bisnis mengajukan permohonan untuk menggunakan platform, harus memberikan semua data identitas yang berkaitan dengan transaksi online kepada operator platform, termasuk nama, waktu pendaftaran, kode identifikasi, kartu identitas, kartu pendaftaran identitas, izin bisnis perusahaan, izin bisnis industri perorangan dan rumah Tangga komersial, sertifikat pendaftaran pajak, izin administratif otorisasi yang diberikan oleh departemen, produsen produk, atau platform jaringan administrasi nasional yang terkait, dan sebagainya). Waralaba, misalnya, dll. serta informasi Otorisasi mencakup konten, waktu, dan otoritas otorisasi. waktu otorisasi, informasi kontak seperti alamat surat, nomor telepon, email, dan pengirim pesan instan, dll. Informasi kontak seperti alamat surat, nomor telepon, email, alat pesan instan, serta data kontak tambahan), dan sebagainya. operator platform elektronikcommerce harus secara ketat meninjau identitas pendaftaran operator platform. sesuai dengan peraturan tinjauan pendaftaran kualifikasi operator platform, dan identitas pengguna operator platform, informasi tentang nama toko, untuk menghindari kebingungan identitas mencegah seseorang mendaftarkan merek dagang, nama perusahaan, dan hak serta kepentingan yang sah lainnya, jangan mengelabui pelanggan. Operator di platform tidak boleh melakukan aktivitas bisnis tanpa izin perusahaan orang lain.

Informasi identitas konsumen harus dipublikasikan. Tidak ada hukum, peraturan, atau standar yang seragam untuk publikasi informasi konsumen. Di dalam Untuk mencapai tujuan konsumsi mereka dalam perdagangan elektronik, pelanggan harus memberikan detail kontak, seperti alamat dan nomor telepon, yang diperlukan kepada penyedia platform. Namun, untuk informasi identitas tambahan bagi Konsumen atau operator e-commerce mungkin tidak memiliki kebutuhan tambahan atau menarik pelanggan untuk memberikan informasi pribadi tambahan kepada operator dengan banyak cara. Tentu saja, untuk operasi e-commerce khusus, ada juga standar sistem nama asli. Namun, operator e-commerce harus memenuhi persyaratan undang-undang ketika mengumpulkan informasi pribadi tentang pelanggan yang penting dan harus persetujuan pelanggan.

Ketiga, secara sah mengumpulkan, menggunakan, dan melindungi data pribadi konsumen. Standar Layanan Platform E-commerce Pihak Ketiga dengan jelas mewajibkan operator untuk melindungi diri platform untuk melindungi pengguna: jika pengguna tidak setuju, operator platform tidak boleh mengungkapkan atau menyebarkan catatan transaksi, daftar pengguna, dan data tambahan kepada pihak ketiga, kecuali jika ditentukan secara berbeda oleh hukum dan ketentuan. Sebagaimana diputuskan oleh Komite Tetap Kongres Rakyat Nasional tentang Pertama, operator e-commerce tidak boleh meningkatkan perlindungan informasi jaringan mencuri atau memperoleh data elektronik pribadi konsumen dengan cara yang melanggar lainnya, dan tidak boleh memberikan atau menjual data elektronik pribadi konsumsi yang melanggar hukum kepada orang lain. Kedua, operator e-commerce di aktivitas yang dilakukan untuk mengumpulkan dan menggunakan data elektronik pribadi konsumen, wajib mengikuti asas sah, sah, dan diperlukan, mengungkapkan tujuan, cara, dan jenis pengumpulan dan penggunaan data, dan dengan persetujuan pengumpulan, harus sesuai dengan peraturan perundang-undangan dan kedua belah pihak mencapai kesepakatan untuk mengumpulkan dan menggunakan informasi. Operator e-commerce harus mengungkapkan peraturan pengumpulan dan penggunaan data. informasi kepada pelanggan saat mengumpulkan dan menggunakan data elektronik mereka. Ketiga, operator e-commerce dan karyawan mereka harus memastikan bahwa mereka benar menjaga kerahasiaan data pribadi pelanggan dalam kegiatan bisnis, dan tidak diizinkan untuk menyebarluaskan, merusak, menjual atau memberikannya kepada orang lain secara ilegal. Keempat, operator e-dagang harus mengambil tindakan teknis dan tambahan yang diperlukan untuk melindungi data dari kebocoran, kerusakan, dan kehilangan informasi elektronik pribadi pelanggan yang dikumpulkan selama operasi perusahaan. Ketika Kebocoran, kerusakan, atau kehilangan data harus diperbaiki segera. dilaksanakan. Kelima, dalam kasus operator e-commerce tidak memberikan data elektronik bisnis kepada orang yang

menerima informasi elektronik, atau orang yang menerima informasi elektronik secara tegas menolak, operator e-commerce dilarang menyampaikan informasi elektronik komersial ke email pribadi, telepon rumah, atau telepon genggam.

Keempat, berpartisipasi dalam kegiatan pemasaran dengan cara yang sah. Untuk terlibat dalam kegiatan pemasaran menurut hukum, diperlukan pertimbangan berikut. Operator yang menyediakan barang atau jasa harus memberikan informasi yang akurat dan lengkap tentang barang atau jasa tersebut. Dalam hal Kementerian Perdagangan mengirimkan pemberitahuan tentang perilaku belanja yang dipromosikan dalam jaringan operator. Dalam mempromosikan barang atau jasa melalui e-commerce, informasi harus diberikan secara Informasi penting tentang barang atau jasa yang dipromosikan secara menyeluruh dan jelas, termasuk nama barang atau jasa, jenis, jumlah, kualitas, harga, pengiriman, distribusi, metode pembayaran, pengembalian, dan sebagainya). Menurut Undang-Undang Peraturan Republik Rakyat Cina tentang Perlindungan Hak Konsumen dan Inter-est, operator e-commerce harus memastikan bahwa tanda barang atau jasa yang dijual oleh mereka untuk memastikan bahwa kebutuhan keselamatan pribadi dan properti dipenuhi. Karena produk atau layanan yang dapat mengancam keselamatan individu dan properti, Selain memberikan penjelasan yang tepat dan petunjuk yang jelas kepada pelanggan, jangan lupa untuk memberikan penjelasan. dan tunjukkan cara mendapatkan barang atau layanan dengan benar dan cara menghindari bahaya. Seandainya operator menemukan bahwa barang atau layanan yang disediakan memiliki kecacatan yang signifikan, dan bahkan jika penerimaan layanan atau penggunaan barang yang tepat masih menyebabkan Operator harus segera melaporkan kerusakan pada keselamatan pribadi atau properti dan memberi tahu departemen administrasi terkait, dan tidak boleh berita palsu, pelanggaran kontrak, dll. Sesuai dengan Standar Layanan Operator platform perdagangan e-commerce pihak ketiga harus mengawasi secara hati-hati dan wajar data transaksi yang dilakukan di platform mereka. Terlibat dalam Dalam aktivitas bisnis di platform, nama dan informasi produsen produk harus publik; dalam kasus di mana lisensi pihak ketiga digunakan, lisensi dan sertifikat sertifikasi juga publikasi diperlukan. Operator stasiun harus menjalankan bisnis mereka secara legal dan tidak boleh melakukan hal lain. menjual barang yang tidak memenuhi persyaratan nasional, beracun atau berbahaya. Informasi tentang produk yang ditunjukkan di halaman web harus orisinal. Kostum fisik (berwujud) harus dapat ditampilkan dari berbagai sudut dan arah, dengan berbagai warna dan ukuran, dan Tidak boleh mengubah atau menampilkan proporsi komoditas; komoditas yang cacat harus dijelaskan secara menyeluruh dan ditunjukkan dengan gambar. Jika operator mengaktifkan Ditemukan bahwa stasiun menyiarkan iklan yang melanggar peraturan, Untuk menghentikannya, operator

harus bertindak cepat. berhenti memberikan mereka platform perdagangan online jika dibutuhkan. Jika bukti dari pengadu dapat menunjukkan bahwa operator telah melakukan pelanggaran atau menyebarkan informasi ilegal di stasiun, operator Platform harus memberi tahu pihak yang bertanggung jawab terkait, menghentikan pelanggaran, pembersihan data yang berbahaya, dan penyebaran data Identitas pengadu dan informasi kontak sesuai permintaan penundaan Operator platform memiliki tanggung jawab untuk memeriksa informasi. secara bijaksana dan logis, menghapus pelanggaran yang jelas atau informasi ilegal tepat waktu dan sesuai dengan hukum, memberi tahu operator stasiun radio.

Operator e-commerce harus meningkatkan legalitas, keamanan, keaslian, dan integritas. ketepatan waktu dan kemudahan menggunakan berbagai informasi bisnis saat didistribusikan dan mengkomunikasikan informasi. Operator e-commerce harus memberikan informasi dengan jujur. barang dan jasa, dan mengungkapkan informasi risiko yang sulit dikonfirmasi dan tidak dapat diantisipasi. Operator platform harus menghindari dan menghentikan data. perdagangan barang ilegal, senjata api, narkoba, dan bahan kimia berbahaya di platform tersebut. Operator e-commerce harus menggunakan platform server secara legal. jaringan, email, iklan jaringan, promosi mesin pencari, dan metode lainnya untuk penerbitan dan distribusi menyampaikan informasi tentang perusahaan. Menghindari dan menghapus tautan berbahaya, gangguan, iklan jaringan tersembunyi, dan strategi publisitas yang salah lainnya. Operator e-commerce harus memberikan layanan informasi yang mudah digunakan dan cepat, update, menghindari, dan hentikan tindakan yang menghalangi pelanggan untuk menanyakan informasi tentang produk, memberikan kebebasan untuk memilih produk, dan menjamin pertukaran informasi yang tepat waktu dan lancar antara pengecer dan konsumen. Bisnis e-commerce haruslah legal, terstandardisasi, adil, dan memiliki perilaku yang adil dalam pemasaran internet.

Operator e-commerce harus menstandarisasi pengembangan anggota dan pendaftaran pengguna. Operator e-commerce harus mendorong konsumen untuk mendaftar dan mengembangkan anggota secara legal, transparan, dan transparan, menghentikan dan mencegah perilaku keanggotaan dengan alasan untuk membayar harga tinggi atau membeli barang, dan menghentikan perilaku penjualan piramida melalui platform online sebagai metode tersembunyi. vendor platform Perdagangan pihak ketiga harus menyediakan layanan yang diperlukan untuk membuka bisnis online dengan pendaftaran nama asli yang diperlukan, pengembangan sistem keamanan dan pencadangan transaksi, serta menemukan dan memperingatkan secara tepat waktu tentang risiko transaksi. Supervisor e Semua bentuk promosi online harus diawasi oleh bisnis, dan melakukan kampanye pemasaran online,

peraturan, tenggat waktu, cakupan produk, dan situasi pembatasan yang terkait dengan pemasaran konten. Menghindari dan menghindari harga asli yang tidak asli, ketidakkonsistenan fisik, dan hadiah yang tidak dikirim dengan cepat dan operasi di belakang layar, serta fenomena lain dalam penjualan online, diskon, dan promosi hadiah online, poin promosi, undian klik, promosi bersama, dan aktivitas lain.

Jangan menjual lotere dengan nilai hadiah maksimum di atas batas legal. Menurut Republik Rakyat Undang-Undang Persaingan Usaha Tidak Sehat Operator Tiongkok tidak boleh menjual hadiah dengan nilai hadiah tertinggi lebih dari 50.000 Yuan.

Mempublikasikan iklan dengan jujur Konten iklan promosi harus benar, legal, jelas, dan mudah dipahami. gambar, atau gambar yang tidak jelas dan menyesatkan, yang menggambarkan situasi imitasi kegiatan promosi, dan menghindari menyebarkan informasi yang tidak benar untuk menipu klien. Informasi iklan yang dikeluhkan harus dihapus oleh operator platform. platform yang bertanggung jawab untuk menangani periklanan administratif sesuai dengan hukum periklanan. Platform transaksi pihak ketiga harus menghalangi operator stasiun untuk menyebarkan informasi iklan yang tidak benar atau mengirimkan email spam. untuk barang atau jasa yang dilarang secara eksplisit oleh negara, platform perdagangan pihak ketiga yang memungkinkan pencarian

membatasi atau menghentikan akses ke nama-nama pada halaman tampilan hasil upaya. Pelanggaran hak kekayaan intelektual, serta pembuatan atau penjualan barang palsu tidak boleh terjadi. Pemberitahuan tentang Perilaku Promosi yang Diatur Kementerian Perdagangan menetapkan belanja online bahwa tidak ada pelanggaran hak kekayaan intelektual, produksi, atau penjualan produk palsu dan buruk dalam promosi.Selain itu, kegiatan pemasaran tidak menghasilkan perilaku penyuapan komersial, data transaksi palsu, atau informasi bisnis palsu.

Kelima, membuat dan mengubah aturan perdagangan platform publisitas sesuai dengan hukuman Aturan Persiapan untuk Aturan Perdagangan Platform Pihak Ketiga menyatakan Regulasi Retail Online (Trial) (Order No. 7, 2014 dari Kementerian Perdagangan), Perdagangan di platform online biasanya mencakup hal-hal berikut: Peraturan dasar Aturan dasar adalah aturan yang dibuat oleh operator. aturan dasar tentang ritel online dan pelanggan pada platform pihak ketiga pembentukan, efisiensi, dan keberhasilan transaksi. Tanggung jawab dan pembagian risiko diatur. Tanggung jawab dan peraturan Pembagian risiko berkaitan dengan peraturan yang diterapkan oleh operator platform pihak ketiga mana yang menanggung tanggung jawab perdata atau membebaskannya aturan pembagian risiko untuk konsumen dan operator ritel online. Peraturan proteksi hak kekayaan intelektual. Peraturan yang memproteksi hak kekayaan intelektual mengarah pada undang-undang yang melindungi hak kekayaan

intelektual dan melarang produk palsu dan berkualitas rendah.Metode evaluasi kredit Dalam aturan evaluasi kredit, aturan yang digunakan oleh operator pihak ketiga platform ritel online untuk menyediakan layanan evaluasi kredit untuk kedua belah pihak, serta pengumpulan, dokumentasi, dan mengungkapkan kondisi kredit masing-masing pihak.Aturan yang Melindungi Konsumen Peraturan yang melindungi hak konsumen dan antar Konsumen berbicara tentang undang-undang yang melindungi hak-hak sah konsumen untuk mengetahui, hak untuk mendapatkan kembali barang dan kompensasi, dan perlindungan informasi pribadi pelanggan dan catatan transaksi. Aturan Pengungkapan Data Regulasi pengungkapan informasi menyatakan bahwa aturan yang digunakan oleh operator platform pihak ketiga untuk mendaftar operator ritel secara online dengan nama asli mereka dan melakukan penilaian kelegalan bisnis mereka. Informasi ilegal dilarang oleh undang-undang. Regulasi untuk menghentikan dan aturan untuk operator platform ritel untuk mencegah informasi ilegal online pihak ketiga untuk menghentikan dan mencegah informasi komoditas didistribusikan dan produk dan iklan di platform mereka yang melanggar ketentuan peraturan perundang-undangan yang berlaku di seluruh negara. Regulasi untuk Penyelesaian Sengketa Transaksi Metode penyelesaian sengketa bisnis menggambarkan prosedur dan peraturan yang digunakan oleh operator platform ritel online pihak ketiga. untuk menyelesaikan konflik antara operator ritel online dan pelanggan. Ketentuan peraturan perdagangan yang berlaku Persyaratan Peraturan Perdagangan mengacu pada persyaratan mengenai subjek, jangka waktu, dan lingkup peraturan perdagangan. Perubahan aturan perdagangan Kriteria perubahan aturan perdagangan mencakup persyaratan prosedur dan cara mengubah dan memodifikasi peraturan yang mengatur perdagangan. Aturan perdagangan tambahan yang diperlukan atau tindakan terkait tertulis. Menurut Pasal 34 Undang-Undang Perdagangan Elektronik, Ketika operator platform perdagangan elektronik melakukan revisi, mereka harus meminta pendapat orang lain. aturan perdagangan platform dan perjanjian layanan di tempat yang menonjol di halaman beranda mereka dan mengambil tindakan yang diperlukan untuk memastikan bahwa pihak-pihak terkait memiliki kesempatan untuk berbicara tepat waktu dan menyeluruh. Sekurang-kurangnya konten yang direvisi harus dipublikasikan. tujuh hari sebelum penerapannya. Jika operator di platform menolak konten yang diubah dan harus dikeluarkan dari platform, operator platform bisnis tidak boleh mencegahnya, dan mereka harus memikul tanggung jawab yang terkait. sesuai dengan aturan transaksi dan perjanjian layanan sebelum modifikasi.

Dalam membuat, mengubah, dan mengembangkan layanan platform e-commerce, penyelenggara harus mematuhi keterbukaan dan keadilan. mematuhi peraturan pemerintah dan hukum, mengatur perdagangan, menghormati etika sosial, dan tidak boleh mengganggu

struktur ekonomi dan sosial serta mengganggu kepentingan publik dan sosial.Keenam, e-commerce harus membangun sistem untuk melindungi data transaksi. dan meningkatkan keamanan jaringan dan sistem data, mengambil tindakan keamanan situs web yang efektif dan kerahasiaan langkah-langkah untuk melindungi data perusahaan dan data pengguna, mencegah dan menghentikan penggunaan internet untuk pencurian rahasia dagang, dan memberikan informasi pengguna kepada pihak ketiga dalam upaya mendapatkan keuntungan. Operator platform e-commerce harus melakukan tindakan yang diperlukan untuk memastikan bahwa platform perdagangan online beroperasi secara normal dan menyediakan lingkungan perdagangan yang aman dan dapat diandalkan serta layanan perdagangan yang adil dan terbuka, menjaga ketertiban perdagangan, dan membangun dan meningkatkan mekanisme peringatan risiko perdagangan dan sistem evaluasi kredit e-commerce, dan memastikan operasi rutin platform e-commerce.

2. Pengendalian risiko dalam transaksi e-commerce

(1) Memperbaiki aturan perdagangan

Operator e-commerce harus membuat perjanjian pengguna yang sah dan adil yang menjelaskan hak dan kewajiban pengguna, dan memastikan bahwa pengguna dapat memahami perjanjian secara menyeluruh sebelum menerimanya. Mencegah dan menghentikan praktik ilegal seperti penipuan dan kolusi jahat untuk mendorong penandatanganan perjanjian. Perusahaan e-commerce harus memberi tahu pengguna terlebih dahulu saat mengubah perjanjian pengguna. Mereka harus menjelaskan alasan perubahan dan konten perubahan.

Sebagai operator bisnis, penyedia layanan lelang dan perdagangan online harus menetapkan standar perilaku bisnis mereka. Selain itu, penyedia layanan harus mematuhi Hukum Lelang Republik Rakyat Tiongkok dan peraturan dan hukum terkait lainnya; secara akurat, jelas, dan lengkap menjelaskan tujuan lelang; dan membuat aturan lelang online yang adil dan masuk akal.

- Perjanjian antara operator platform e-commerce dan pengguna. Menurut ketentuan yang relevan dari Standar Layanan untuk Pihak Ketiga Platform Perdagangan E-commerce pihak ketiga, perjanjian pengguna dan modifikasi operator platform harus diumumkan 30 hari sebelumnya. Kopinya harus dikirim ke lembaga lokal yang melindungi hak dan kepentingan konsumen jika melibatkan hak dan kepentingan konsumen. Perjanjian pengguna harus mencakup hal-hal berikut: persyaratan pendaftaran pengguna; aturan perdagangan; perlindungan privasi dan rahasia dagang; dan prosedur modifikasi protokol pengguna. Kelima, pendekatan penyelesaian perselisihan. Keenam, yurisdiksi dan

perjanjian tertentu yang diatur oleh hukum Tiongkok. Ketujuh, tanggung jawab yang terkait.

Operator platform harus menggunakan metode teknis dan lainnya untuk memastikan bahwa pengguna memahami perjanjian pengguna secara menyeluruh, termasuk risiko transaksi yang wajar, pembatasan tanggung jawab, dan klausul pembebasan tanggung jawab. Namun, mereka tidak boleh membebaskan diri dari tanggung jawab mereka, memperberat kewajiban mereka, atau menghilangkan hak-hak hukum pengguna.

Selama masa cooling-off, operator platform dapat mengatur waktu istirahat sistem. Ini memungkinkan pelanggan membatalkan pesanan mereka tanpa alasan apa pun.

- Kontrak antara operator platform dan operator dalam bentuk platform. Menurut Standar Layanan untuk Perdagangan Elektronik Pihak Ketiga Platform Perdagangan, operator platform harus menetapkan hak dan kewajiban yang relevan, tanggung jawab atas pelanggaran kontrak, dan metode penyelesaian perselisihan yang sesuai dengan hukum ketika mereka menandatangani kontrak operasi masuk. Kontrak tersebut harus berisi syarat dan ketentuan yang diperlukan berikut ini: Pertama, operator platform dan operator stasiun tidak boleh merugikan kepentingan negara dan publik dalam transaksi komoditas jaringan dan perilaku layanan terkait, tidak membahayakan hak dan kepentingan konsumen yang sah; kedua, operator stasiun harus mematuhi prinsip-prinsip dasar kejujuran dan kepercayaan, disiplin diri yang ketat, untuk melindungi kepentingan nasional, untuk memikul tanggung jawab sosial, transaksi online dengan cara yang jujur, adil, sehat, dan teratur, mereka tidak boleh menggunakan transaksi online untuk terlibat dalam kegiatan ilegal atau kriminal; Ketiga, operator telekomunikasi harus memperhatikan untuk mengawasi informasi yang dikeluarkan oleh pengguna, menghapus informasi yang melanggar peraturan negara sesuai dengan hukum, menjaga dan mengurangi spam; keempat, operator bisnis di stasiun harus membuat sistem yang relevan untuk mediasi dan penanganan perselisihan transaksi pasar, dan dalam posisi yang menonjol dari lembaga penanganan perselisihan dan informasi kontak.

(2) Peserta transaksi e-commerce harus menandatangani kontrak sesuai dengan hukum

- Dalam transaksi e-commerce, pihak-pihak yang bertransaksi disarankan untuk menyimpulkan kontrak sesuai dengan Hukum Tanda Tangan Elektronik Republik Rakyat Tiongkok. Untuk transaksi online dengan jumlah target lebih dari 50.000 RMB, platform perdagangan pihak ketiga harus meminta kedua belah pihak untuk menggunakan tanda tangan elektronik, menurut Standar Layanan untuk Platform Perdagangan E-commerce Pihak Ketiga.

- Operator peron harus mengeluarkan kredensial transaksi. Operator peron harus meminta operator transaksi di stasiun untuk mengeluarkan kartu voucher, dokumen layanan, dan voucher yang relevan. Hukum faktur elektronik berdampak serupa dengan hukum faktur kertas konvensional.

(3) Tidak akan terlibat dalam transaksi ilegal yang dilarang oleh hukum

- Jujur, dapat dipercaya, dan sangat disiplin diri. Semua orang yang melakukan transaksi e-commerce harus menjadi jujur dan dapat dipercaya, memiliki disiplin diri yang ketat, dan melakukan transaksi online dengan cara yang sehat dan tertib. Mereka juga tidak boleh menggunakan transaksi online untuk terlibat dalam kegiatan ilegal atau kriminal.
- Operator platform e-commerce tidak boleh terlibat dalam transaksi yang melanggar peraturan, hukum, atau kebijakan.
- Operator perdagangan elektronik tidak boleh melakukan tindakan yang tidak sehat terhadap persaingan. Menurut Standar Layanan untuk Platform Perdagangan E-commerce Pihak Ketiga, Undang-undang Perdagangan Elektronik Pasal 22, platform perdagangan pihak ketiga yang menggunakan platform mereka sendiri untuk memperdagangkan barang atau jasa secara online tidak boleh berkolusi satu sama lain, menggunakan kenyamanan mereka sendiri untuk memanipulasi harga pasar, mengganggu ketertiban pasar, atau merusak hak-hak yang sah dan kepentingan operator lain atau konsumen. Pada saat yang sama, tidak ada perilaku persaingan tidak sehat seperti evaluasi kredit yang dilakukan oleh manusia. Operator platform tidak boleh meningkatkan reputasi perusahaan mereka untuk diri mereka sendiri, orang lain, atau melalui orang lain dengan cara transaksi fiktif, menghapus ulasan negatif, atau merusak reputasi pesaing. Operator platform harus meningkatkan pengawasan dan pemrosesan. Operator e-commerce tidak boleh terlibat dalam persaingan yang tidak sehat, seperti menyikat inventaris.
- Operator e-commerce diwajibkan untuk mematuhi kebijakan, undang-undang, dan peraturan yang berkaitan dengan perlindungan hak kekayaan intelektual.
- Perilaku transaksi yang merugikan pelanggan: Pelanggan tidak boleh melakukan transaksi yang curang, menyalahgunakan wewenang, membeli barang dengan harga murah, dan lain-lain.

(4) Pengendalian risiko pembayaran

- Lembaga pembayaran memenuhi syarat untuk menjadi legal. Pembayaran elektronik harus dilakukan oleh bank atau non-bank. institusi pembayaran yang memiliki kualifikasi hukum.

- Kami akan meningkatkan standar teknis dan bisnis pembayaran online. China terus memperluas sistem pembayaran online. Mempelajari langkah-langkah pencegahan risiko, meningkatkan pengawasan bisnis dan pengendalian risiko; secara aktif mempelajari peraturan yang relevan dari layanan pembayaran pihak ketiga, membantu bank komersial dan China UnionPay membangun platform pembayaran elektronik yang aman, cepat, dan nyaman; meningkatkan sistem kliring dana online, mendorong standarisasi dan standarisasi bis untuk mendorong lembaga layanan pembayaran untuk mengembangkan metode pembayaran elektronik yang aman dan mudah digunakan untuk memenuhi kebutuhan pembayaran elektronik yang beragam. Untuk mengurangi biaya penyelesaian dan pembayaran, meningkatkan efisiensi perputaran modal, dan menjamin keamanan kata sandi dan data pembayaran, platform pembayaran elektronik harus mengambil tindakan yang efektif.
- Ada kemungkinan pembayaran transaksi yang cepat dan tepat waktu. Operator platform e-commerce harus memberi tahu pelanggan tentang risiko transaksi dan meminta mereka untuk memverifikasi detail transaksi sebelum melanjutkan proses pembayaran; lembaga pembayaran; dan konsumen harus lebih sadar keamanan dan pengetahuan teknis tentang pembayaran online untuk menghindari risiko.

Meskipun metode pembayaran cash on delivery tidak selalu berlaku, operator e-commerce bertanggung jawab untuk mengelola risiko pembayaran. Pertama, metode pembayaran ini pada dasarnya terbatas pada platform yang dioperasikan sendiri; operator platform e-commerce pihak ketiga pada dasarnya tidak menggunakan metode pembayaran cash on delivery untuk mengendalikan risiko uang tunai atas barang. Kedua, metode pembayaran ini tidak dapat digunakan untuk barang-barang mahal seperti printer dan ponsel, dan dimaksudkan untuk konsumsi kecil. Terakhir, operator platform dapat memasukkan pelanggan dengan peringkat kredit buruk ke dalam daftar hitam pembayaran tunai saat pengiriman dengan menambahkan sistem evaluasi peringkat kredit mereka.

(5) Pengendalian risiko logistik dan distribusi

- memberi tahu orang tentang distribusi secara langsung. Perusahaan e-commerce dapat mengumumkan informasi distribusi secara real-time melalui situs web permintaan informasi, pemberitahuan email, pemberitahuan telepon, dan metode ampuh lainnya, sambil menjelaskan prosedur dan waktu pengiriman. Perusahaan e-commerce ketat mematuhi pesanan barang dan perjanjian transaksi. Mereka juga menghindari penundaan pengiriman, ketidaksesuaian fisik, biaya pengiriman tambahan, dan tindakan lainnya. Menganjurkan perusahaan e-commerce untuk berusaha berkolaborasi dengan pembeli

mengenai pengiriman barang untuk melindungi hak konsumen untuk pengetahuan dan keputusan.

- Meningkatkan sistem logistik. Perusahaan e-commerce harus membangun platform layanan logistik pihak ketiga, secara bertahap menciptakan komunitas distribusi logistik yang terintegrasi dan profesional untuk pedagang online, membangun sistem jaringan distribusi logistik yang mencakup berbagai industri, dan meningkatkan responsifitas dan efisiensi distribusi.
- Menjaga agar data pribadi tidak tersebar luas. Perusahaan logistik dapat menggunakan "lembar privasi" untuk menghindari data pelanggan dibocorkan.

(6) Menyimpan catatan transaksi

- Untuk melacak dan menyimpan transaksi, operator perdagangan elektronik harus membuat sistem. Menurut Spesifikasi Mode Perdagangan Elektronik, operator perdagangan elektronik harus membuat sistem pencatatan dan penyimpanan yang aman dan dapat diandalkan untuk transaksi, menyimpan informasi pendaftaran pengguna, dan mencatat transaksi data selama setidaknya 10 tahun, kecuali ditentukan lain oleh hukum dan peraturan administratif. Sistem dan langkah-langkah keamanan harus diambil untuk melindungi hak privasi kedua belah pihak.
- Memberikan layanan untuk penyimpanan dan permintaan data Operator platform harus memastikan perlakukan penyimpanan semua informasi transaksi dan layanan yang dirilis di platform, serta mengambil langkah teknis yang sesuai untuk memastikan integritas, keakuratan, dan keamanan data di atas, menurut Standar Layanan untuk Platform Perdagangan E-commerce Pihak Ketiga. Data operator dan mitra transaksi yang ditemukan di platform tidak boleh disimpan lebih dari dua tahun sejak tanggal login terakhir; selain itu, data transaksi tidak boleh disimpan lebih dari dua tahun sejak tanggal kejadian. Selama periode penyimpanan, operator platform harus memiliki hak untuk meminta, mengunduh, atau mencetak informasi transaksi mereka sendiri. Untuk memasarkan data mereka, platform perdagangan pihak ketiga harus menggunakan agen layanan data independen. Mereka juga dapat menawarkan layanan permintaan, pengunduhan, atau pencetakan dari pihak ketiga. Pasal 31 UU Perdagangan Elektronik menetapkan bahwa penyelenggara platform perdagangan elektronik harus mencatat dan menyimpan informasi tentang komoditas dan layanan serta informasi tentang transaksi yang dipublikasikan di platform tersebut untuk menjamin integritas, kerahasiaan, dan aksesibilitas informasi tersebut. Informasi tentang barang dan jasa serta transaksi harus disimpan tidak lebih dari tiga tahun

sejak tanggal transaksi, kecuali jika ditentukan lain oleh undang-undang atau peraturan administratif.

(7) Operator platform e-commerce harus mengawasi aktivitas perdagangan sesuai dengan hukum dan peraturan

- Jika operator platform e-commerce terlibat dalam tindakan ilegal, operator platform dapat menangguhkan atau menghentikan transaksi. Sesuai dengan prosedur yang diumumkan sebelumnya, operator perdagangan elektronik platform dapat mempublikasikan operator yang terlibat dalam operasi ilegal atau pelanggaran hak dan kepentingan konsumen di platform.
- Pemilik platform e-commerce harus meningkatkan pengawasan mereka sendiri dan mengurangi risiko perdagangan. Platform e-commerce, khususnya platform utama, harus membentuk mekanisme pengawasan internal dan secara teratur memeriksa perusahaan perdagangan internasional dengan itikad baik, melindungi hak kekayaan intelektual, meningkatkan file kredit internal, membuat pengingat internal, pembatasan lokal dan pembatasan lengkap, dan secara aktif menangani pengaduan dan laporan. Selain itu, mereka harus menghentikan kolaborasi dengan perusahaan yang melakukan kegiatan ilegal seperti penyelundupan, penggelapan mata uang, dan penyelundupan.
- Operator platform e-commerce harus membuat sistem untuk memantau penjualan barang yang mencurigakan. Operator perdagangan elektronik harus membentuk tim pemantau khusus untuk memantau informasi penjualan komoditas. Tim pemantau harus berkonsentrasi pada memantau penjualan barang selundupan, barang murah, dan konten lainnya. Segera laporkan situasi mencurigakan ke departemen terkait untuk penyelidikan dan penanganan. Perdagangan online.

3. Pengendalian risiko setelah transaksi e-commerce

(1) Menerapkan layanan purna jual dan sistem pengembalian dan penukaran sesuai dengan hukum

- Operator e-commerce harus menetapkan, meningkatkan, merilis, dan menerapkan secara ketat layanan purna jual serta sistem penukaran dan pengembalian. Ini mencegah tanggung jawab purna jual, mencegah penundaan penggantian, dan mencegah barang yang dikembalikan, dan melindungi hak dan kepentingan yang sah pelanggan yang membeli barang online.
- Gunakan sistem yang ketat untuk pengembalian barang tanpa alasan selama tujuh hari. Undang-Undang Republik Rakyat Tiongkok tentang Perlindungan Hak dan Kepentingan Konsumen mengatur sistem ini. Konsumen memiliki hak untuk mengembalikan barang

yang dijual oleh operator komoditas jaringan dalam waktu tujuh hari sejak tanggal penerimaan barang, kecuali barang-barang berikut: pertama, barang yang disesuaikan oleh konsumen; kedua, barang yang masih baru dan mudah rusak; ketiga, barang digital seperti produk audio dan visual serta perangkat lunak komputer yang dimuat secara online atau tidak disegel oleh konsumen; dan keempat, koran dan majalah yang dikirimkan. Selain barang yang disebutkan di atas, barang lain yang sesuai dengan sifat barang dan telah dikonfirmasi oleh pelanggan tidak dapat dikembalikan tanpa alasan. Ketika pelanggan mengembalikan barang, barang harus dalam kondisi baik. Dalam waktu tujuh hari sejak tanggal barang yang dikembalikan, operator barang online harus mengembalikan harga barang yang telah dibayarkan oleh pelanggan. Konsumen akan bertanggung jawab atas biaya pengiriman barang yang dikembalikan. Jika operator komoditas jaringan dan konsumen menyetujui sebaliknya, perjanjian tersebut akan berlaku.

- Platform perdagangan elektronik harus memenuhi tanggung jawab mereka sesuai dengan peraturan negara bagian. Operator platform perdagangan elektronik harus mewajibkan platform operator bentuk melalui kontrak atau cara lain untuk mematuhi ketentuan yang relevan di negara bagian. Mereka juga harus menjalankan layanan purna jual komoditas dan sistem pengembalian tanpa melanggar ketentuan layanan purna jual komoditas dan sistem pengembalian operator stasiun. Operator platform juga harus menangani keluhan konsumen dan bertanggung jawab atas keluhan konsumen.

(2) Menetapkan sistem margin penjual

- Operator platform e-commerce harus memberikan layanan "margin penjual" kepada pelanggan, menurut Spesifikasi Layanan untuk Platform Perdagangan E-commerce Pihak Ketiga. Ketika pelanggan mengalami kerugian dalam transaksi, deposit penjual digunakan sebagai kompensasi. Terlebih dahulu, departemen administrasi lokal untuk industri dan perdagangan harus diberitahu tentang jumlah dan cara deposit penjual digunakan. Jika operator platform perdagangan elektronik dan operator di dalam platform setuju untuk mengatur deposit hak dan kepentingan konsumen, kedua belah pihak harus membuat perjanjian yang jelas tentang jumlah, manajemen, penggunaan, dan pengembalian deposit hak dan kepentingan konsumen menurut Pasal 58 Undang-Undang Perdagangan Elektronik. Untuk konsumen, Undang-Undang Republik Rakyat Tiongkok tentang Perlindungan Hak dan Kepentingan Konsumen akan berlaku. Undang-undang ini menetapkan bahwa operator platform e-commerce harus membayar konsumen dan memberikan kompensasi kepada operator platform e-commerce.

(3) Menangani sengketa transaksi secara aktif

- Operator e-commerce harus membuat sistem pengaduan dan pelaporan yang mudah dan efektif, mengungkapkan informasi tentang pengaduan dan prosedur pelaporan, dan menerima dan menangani keluhan dan laporan secara tepat waktu.
- Operator platform e-commerce harus bertindak sebagai supervisi platform. Mereka harus menangani tindakan bisnis operator platform yang melanggar hukum dan peraturan nasional sesuai dengan peraturan dan hukum yang berlaku. Operator platform e-commerce harus memberikan informasi pendaftaran situs web yang sebenarnya kepada konsumen dari operator di platform jika konsumen membeli barang atau menerima layanan di platform tersebut, dan secara aktif membantu konsumen untuk melindungi hak dan kepentingan mereka yang sah. Operator platform e-commerce juga harus menyelidiki dan memverifikasi keluhan kesalahan operasional yang diajukan oleh konsumen terkait dengan platform tersebut. Menurut Pasal 63 UU PMSE, penyelenggara platform e-commerce diizinkan untuk membuat mekanisme penyelesaian sengketa secara online, membuat dan mempublikasikan peraturan untuk penyelesaian sengketa, dan menyelesaikan sengketa antara pihak secara adil dan tidak memihak sesuai dengan prinsip pelayanan sukarela.
- Jika ada perselisihan antara pelanggan dan operator e-commerce mengenai barang dan jasa, operator e-commerce harus menanggung tanggung jawab pembuktian hukum bagi pelaku bisnis, dan konsumen harus membuktikan bahwa ada bukti kerusakan. Sengketa diselesaikan menurut peraturan perundang-undangan yang berlaku. Untuk menyelesaikan sengketa e-commerce, pelaku usaha e-commerce harus menyerahkan kontrak dan bukti transaksi yang asli, menurut Pasal 62 UU ITE. Penyelenggara perdagangan elektronik akan bertanggung jawab secara hukum jika mereka menghilangkan, memalsukan, merusak, menghancurkan, menyembunyikan, atau menolak untuk memberikan informasi yang disebutkan di atas. Jika ini menyebabkan pengadilan, lembaga arbitrase, atau organ terkait menemukan informasi tersebut, penyelenggara perdagangan elektronik akan bertanggung jawab secara hukum.
- Kewajiban dan kolaborasi operator e-commerce Operator platform harus bekerja sama secara tepat waktu untuk menangani pengaduan sengketa transaksi online melalui mekanisme pengaduan online yang diterima oleh asosiasi konsumen dan organisasi terkait. Sesuai dengan prosedur dan aturan yang diumumkan sebelumnya, operator platform dapat membatasi akses pasar operator stasiun untuk pengguna yang nakal. Untuk menangani masalah konsumen atau pihak ketiga, operator platform harus bekerja sama dengan operator platform. Penyelenggara usaha rumah susun harus berusaha bekerja sama dengan penyelenggara usaha platform untuk menyelidiki dan mengatur pengaduan konsumen.

Pasal 61 UU PMSE menetapkan bahwa penyelenggara platform e-commerce harus secara aktif membantu pelanggan untuk melindungi hak-hak dan kepentingan yang sah mereka ketika pelanggan membeli barang atau layanan pada platform e-commerce dan kemudian muncul perselisihan dengan penyelenggara platform.

4. Pengendalian teknis atas risiko transaksi

Operator platform e-commerce harus mematuhi persyaratan keamanan tingkat informasi nasional dan persyaratan konstruksi, operasi, dan pemeliharaan sistem platform perdagangan online, serta memastikan bahwa semua fasilitas perangkat keras dan perangkat lunak di platform perdagangan berfungsi dengan baik, serta menjaga fasilitas pengendalian kebakaran, kesehatan, dan keamanan dalam kondisi normal. Menurut Standar Layanan untuk Platform Perdagangan E-niaga Pihak Ketiga, platform dengan omset harian lebih dari 100 juta yuan (termasuk 100 juta yuan) harus memiliki sistem cadangan bencana jarak jauh dan sistem rencana darurat dan pemulihan bencana.

6.3.3 Peraturan Pasar

Pengawasan pasar adalah pengaturan dan pembatasan entitas bisnis e-commerce untuk mencapai tujuan kebijakan publik seperti keamanan transaksi.

1. Ideologi yang memandu pengawasan pasar

Pasar regulator harus berkonsentrasi pada menciptakan lingkungan yang baik untuk akses, persaingan, dan konsumsi. Mereka harus membangun konsep dan mekanisme pengawasan pasar yang kontemporer, mereformasi sistem yang ada, mengembangkan mekanisme baru, meningkatkan pengetahuan dan efisiensi, dan mendorong pembangunan ekonomi dan masyarakat yang sehat dan berkelanjutan. Aspek-aspek berikut menunjukkan filosofi panduan pengawasan pasar.

Untuk memulai, kami akan meningkatkan vitalitas pasar. Faktor penting yang mendorong pertumbuhan ekonomi yang berkelanjutan dan kemakmuran ekonomi adalah sifat internal ekonomi pasar. Kita perlu mengubah definisi konvensional dari "manajemen" dan menjadikan stimulasi pertumbuhan dan inovasi pasar sebagai tujuan penting dari regulasi pasar.

Kedua, kami akan menetapkan struktur pasar. Ekonomi pasar yang sehat tidak hanya teratur, tetapi juga selalu berubah. Ekonomi pasar kehilangan vitalitasnya dan keamanannya jika tidak ada ketertiban. Regulasi pasar harus berfokus pada pengaturan tatanan pasar dan menjaga persaingan yang sehat, menggabungkan deregulasi dengan regulasi yang baik, dan memastikan bahwa deregulasi dilakukan dengan cara yang teratur dan konsisten.

Ketiga, kami akan melindungi hak dan kepentingan konsumen. Untuk mewujudkan pembangunan bersama, kita harus mengutamakan konsep konsumen, menempatkan perlindungan hak dan kepentingan konsumen sebagai dasar regulasi pasar, dan meningkatkan kepuasan masyarakat dan keuntungan.

Keempat, kami bermaksud meningkatkan efektivitas regulasi. Untuk meningkatkan efisiensi operasi pasar, kita harus meningkatkan efisiensi pengawasan pasar. Kita harus meningkatkan pemahaman tentang biaya, meningkatkan pemahaman tentang efisiensi sebagai persyaratan dasar, mengubah gagasan tentang pengawasan pasar tak terbatas, mengubah metode yang ditargetkan dan universal, dan mendorong reformasi dan inovasi.

Kelima, kami akan meningkatkan visi internasional kami. Dalam proses globalisasi ekonomi, gagasan tentang pengawasan pasar dan metode yang digunakan telah menjadi komponen penting yang mempengaruhi daya saing nasional dan pengaruh internasional. Ini sejalan dengan tren globalisasi pembangunan ekonomi nasional, seiring dengan kebutuhan untuk meningkatkan kekuatan legislatif negara dalam tata kelola global, untuk mempelajari perumusan aturan peraturan pasar dan dampak pengawasan pasar dan penegakan hukum dari sudut pandang internasional, dan untuk terus meningkakan jumlah uang yang dikeluarkan oleh pasar.

2. Prinsip-prinsip utama regulasi pasar

Pertama, prinsip pengawasan harus sesuai dengan hukum. Semua entitas pasar akan diperlakukan dengan adil dan setara sesuai dengan hukum dan peraturan, dan kami akan melindungi hak dan kepentingan yang sah mereka. Dengan menggunakan pemikiran negara hukum dan metode tugas pengawasan pasar, sistem manajemen menciptakan daftar implementasi penuh, kekuasaan tanpa otorisasi, daftar tanggung jawab yang jelas harus dilakukan, daftar negatif yang jelas dilarang, tidak ada dasar hukum yang tidak dapat diperiksa, menstandarisasi kebijaksanaan pemerintah, mendorong standarisasi pasar, dan supremasi hukum.

Kedua, prinsip dasar pengawasan Desentralisasi, pipa, peraturan yang sederhana dan efisien, overhead "Jane", mengoptimalkan persyaratan reformasi layanan, menghilangkan peraturan yang tidak perlu, sistem yang ketinggalan jaman, aturan yang tidak dapat direalisasikan, mengurangi beban perusahaan, dan mengurangi biaya sosial.

Ketiga, prinsip pengawasan ketat Kami akan mempelajari cara yang ilmiah dan efektif untuk menerapkan regulasi, menerapkan regulasi yang inklusif, mereformasi model regulasi tradisional, dan mendorong pertumbuhan dan kemakmuran ekonomi inovatif. Kami akan melakukan ini untuk menanggapi tren baru dalam teknologi, industri, bentuk bisnis, dan model

bisnis yang berkembang dengan cepat. Untuk menghilangkan bahaya dan risiko tersembunyi, kita harus secara ketat mengawasi area dengan potensi risiko tinggi dan risiko sosial yang tinggi.

Prinsip keempat dari pengaturan yang komprehensif Jika kita ingin beradaptasi dengan tren umum dalam inovasi ilmiah dan teknologi, integrasi industri, dan pembangunan lintas batas, kita harus mengatasi masalah timbal balik, penegakan hukum berganda dan standar yang berbeda, mendorong penegakan hukum yang komprehensif dalam pengawasan pasar, membangun sistem visi super, dan memanfaatkan semua sumber daya peraturan. Kami akan meningkatkan pertukaran informasi, meningkatkan koordinasi di antara semua departemen, dan membangun mekanisme kerja sama dan respons lintas departemen dan regional yang efektif untuk penegakan hukum. Tujuan kami adalah untuk mengurangi titik buta peraturan dan mengurangi biaya penegakan hukum.

Kelima, dasar peraturan yang cerdas. untuk menyesuaikan diri dengan tren baru dalam revolusi ilmiah dan teknologi dan transformasi industri, memenuhi persyaratan langsung dari pengembangan entitas pasar, dan memberikan peran penuh pada peran ilmu pengetahuan dan teknologi dalam regulasi pasar. Untuk mendorong inovasi regulasi, kami akan menggunakan data besar; kami akan menggunakan Internet dan teknologi data besar untuk membangun platform data besar untuk regulasi pasar, mendorong "regulasi Internet plus," dan meningkatkan tingkat regulasi pasar yang cerdas.

Keenam, prinsip pengawasan yang sistematis. Pengawasan pasar harus mengubah cara konvensional di mana pemerintah mengambil semua tanggung jawab, memperjelas tanggung jawab utama perusahaan, mendorong entitas pasar untuk menahan diri dan beroperasi dengan integritas, dan menghilangkan efek dari "pemerintah mendesak, perusahaan tidak mendesak" dan "konsumen tidak berdaya, operator tidak takut". berikan perhatian penuh pada fungsi pengikatan sistem kredit, organisasi industri yang disiplin diri, dan organisasi konsumen, serta opini publik, dalam membangun tata kelola sosial.

3. Organisasi pengawasan pasar

Untuk mencapai tujuan pengawasan pemerintah, perlu memenuhi tugas dari semua departemen dan pemerintah daerah di semua tingkatan, mendorong semua entitas pasar, konsumen, bisnis, dan organisasi di media sosial untuk bekerja sama dan membentuk sinergi dalam pengawasan pasar.

Pertama, meningkatkan koordinasi dan organisasi. Untuk mendukung reformasi dan pembangunan, semua departemen pemerintah dan pemerintah daerah harus mengubah cara mereka berpikir, meningkatkan kesadaran, dan memperkuat dan meningkatkan pengawasan

pasar. Mereka juga harus benar-benar memahaminya. Untuk mencapai tujuan kami, kami akan membangun sistem pertemuan antar kementerian untuk pengawasan pasar, memperkuat organisasi dan kepemimpinan, mempertahankan koordinasi yang erat, meningkatkan mekanisme kerja, meningkatkan koordinasi departemen dan hubungan antara tingkat atas dan bawah, dan mengoordinasikan dan mempromosikan tugas dan rencana reformasi yang jelas.

Kedua, jelaskan bagaimana tanggung jawab dibagi. Semua departemen harus meningkatkan rasa tanggung jawab, mendefinisikan situasi secara keseluruhan, melaksanakan tanggung jawab masing-masing, bekerja sama dengan erat, memperjelas jadwal dan rute, dan terus mendukung pelaksanaan rencana. Pemerintah daerah di semua tingkatan harus benar-benar mengubah perspektif mereka, mengakui pengawasan pasar sebagai cara penting untuk meningkatkan ekonomi lokal dan mempromosikan kemakmuran dan pertumbuhan ekonomi lokal, dan memasukkan tujuan dan tanggung jawab perencanaan ke dalam rencana kerja pemerintah. Organisasi sosial dan asosiasi perdagangan yang relevan harus berpartisipasi secara aktif dalam proses perencanaan, berpartisipasi dalam inisiatif, dan bertindak sesuai dengan persyaratan. Kita harus memberikan perhatian penuh kepada komite ahli pengawasan pasar dan para ahli serta cendekiawan yang relevan; memperkuat wadah pemikir untuk kebijakan komparatif; meningkatkan penelitian teoritis dan penelitian penanggulangan; dan mendorong penelitian ilmiah dan demokratisasi proses pengambilan keputusan.

4. Tujuan dan tugas utama pengawasan pasar

Regulasi pasar berfokus pada membangun sistem pasar modern yang terbuka, teratur, berintegritas, dan peraturan yang kuat, menyempurnakan kerangka kerja bisnis, meningkatkan sistem kebijakan persaingan, dan membangun sistem pengawasan pasar yang ilmiah dan efisien. Sistem ini dibangun berdasarkan supremasi hukum, disiplin perusahaan, dan dukungan sosial untuk pola regulasi pasar yang baru, yang mendorong inovasi kewirausahaan, integritas, dan lingkungan yang aman.

1. Tujuan khusus pengawasan pasar

- Untuk menciptakan lingkungan akses pasar yang tenang dan nyaman. Kami akan meningkatkan sistem akses pasar dan membentuk aturan akses pasar induk yang adil, terpadu, terbuka, dan transparan. Semua jenis persetujuan administratif dan tinjauan telah berkurang, item yang diperiksa dan disetujui sebelum dan sesudah pendaftaran komersial telah berkurang, dan semua izin dan lisensi yang tidak perlu pada dasarnya dibatalkan.
- membuat persaingan pasar yang teratur dan adil. Kami menetapkan regulasi pasar nasional yang terpadu untuk menghilangkan pengawasan dan penegakan hukum yang berulang-

ulang, sehingga pasar nasional semakin terintegrasi. Penegakan hukum anti monopoli dan anti persaingan tidak sehat telah berkembang pesat. Pelanggaran dan pemalsuan telah dilarang, monopoli dan perlindungan industri lokal telah dilindungi, tatanan pasar telah ditingkatkan, peran merek dan merek telah dimainkan sepenuhnya, dan kualitas entitas pasar telah ditingkatkan.

- memberikan lingkungan yang aman dan aman untuk konsumen di pasar. Konsumen telah melihat peningkatan sistem hukum yang melindungi hak-hak mereka. Hak-hak konsumen telah diperkuat. Pada dasarnya, hak-hak konsumen telah dilindungi, dan jaringan pengaduan dan laporan konsumen yang terintegrasi di seluruh negeri telah dibangun. Ketika asosiasi konsumen dan kelompok konsumen lainnya menjadi lebih kuat, hak dan kepentingan konsumen telah dilindungi dengan lebih baik. Konsumen terus menjadi lebih puas, dan kualitas dan keamanan barang dan jasa telah meningkat.
- Kami akan membangun sistem pengawasan pasar yang sah dan efektif. Kami akan mereformasi sistem penegakan hukum pengawasan pasar secara keseluruhan, meningkatkan metode pengawasan pasar, dan membentuk pengawasan pasar dan sistem penegakan hukum anti-monopoli yang terpadu dan terstandardisasi dengan hak dan tanggung jawab yang jelas, efisiensi dan keadilan, dan jaminan supremasi hukum. Pengawasan kredit, pengawasan big data, dan multi-governance mulai muncul.

2. Tugas-tugas utama pengawasan pasar

- Kami akan membuat lingkungan akses pasar yang tenang dan menyenangkan. Kami akan mengubah sistem tinjauan dan persetujuan administratif, mengubah fungsi pemerintah, dan mengurangi tinjauan dan persetujuan administratif. Kami juga akan mendorong masyarakat untuk berwirausaha dan berinovasi, mendorong pertumbuhan entitas pasar yang berkelanjutan dan cepat, dan menyuntikkan vitalitas dan dorongan baru ke dalam pembangunan ekonomi. Secara khusus, mencakup: Kami akan mengubah mekanisme akses pasar. Pertama-tama, kami akan mempermudah akses pasar. Kami akan mereformasi beberapa batasan pemeriksaan dan persetujuan, membangun sistem akses pasar yang terintegrasi, terbuka, dan transparan, dan menciptakan lingkungan di mana investasi dan kewirausahaan dapat dilakukan dengan adil. Kami akan membuat dan memperbaiki sistem daftar negatif untuk mendapatkan akses ke pasar. Kedua, reformasi "lisensi dulu baru kemudian" akan diperdalam. Kami akan mengubah konsep konvensional tentang "ekonomi pemeriksaan dan persetujuan", serta mengurangi semua jenis izin produksi, izin usaha, dan kualifikasi, dan mengurangi luasnya persetujuan dan pemeriksaan pemerintah. Kami akan

meningkatkan reformasi, terus mengurangi pra- dan pasca-persetujuan pendaftaran komersial, dan menyelesaikan perbedaan antara mendapatkan lisensi mudah dan sulit. Kami akan membuat pemeriksaan dan persetujuan lebih mudah, terintegrasi, dan standar. Proyek investasi, menerapkan pemeriksaan dan persetujuan paralel secara online, mengklarifikasi standar, mempersingkat proses, dan menyelesaikannya dalam waktu yang singkat.

Kami akan melanjutkan reformasi sistem registrasi perusahaan. Pertama, kami akan melakukan reformasi dengan menggabungkan lebih dari satu sertifikat. Untuk meningkatkan efisiensi investasi sosial dan kewirausahaan, kami akan mengubah prosedur pemeriksaan, persetujuan, dan pengelolaan entitas pasar dari berbagai departemen. Kedua, kami akan meningkatkan layanan. Kami akan mengubah sistem persetujuan nama perusahaan agar mereka dapat memilih nama sendiri. membuat perubahan nama perusahaan lebih mudah dan lebih efisien. Kami akan membuat prosedur untuk menangani perselisihan nama perusahaan, memperbaiki prosedur untuk menyelesaikan konflik antara nama perusahaan dan merek dagang terdaftar dan merek dagang terkenal lainnya, dan melindungi hak dan kepentingan perusahaan yang sah. memperkuat sistem koreksi wajib untuk nama yang tidak pantas dan memastikan ketertiban umum dan kebiasaan baik. Kami akan memperbaiki dan menghapus pembatasan yang tidak masuk akal dalam sistem pendaftaran grup perusahaan. Kami akan meningkatkan aplikasi dan fasilitasi serta mempercepat seluruh proses pendaftaran perusahaan secara elektronik. Kami akan mendukung reformasi izin usaha elektronik percontohan dan memperluas cakupannya. Ketiga, untuk mendukung gelombang kreativitas dan kewirausahaan. Kami akan mendukung kewirausahaan dan inovasi serta memperbaiki sistem registrasi bisnis. Keempat, memastikan bahwa pendaftaran perusahaan tetap independen.

Kami akan meningkatkan proses keluar dari bisnis. Pertama-tama, Tingkatkan metode pembatalan dasar. Sederhanakan dan tingkatkan proses pembatalan bisnis dan individu, serta ciptakan mekanisme keluar pasar yang mudah dan teratur. Kedua, membuat sistem keluar yang diperlukan. Kami akan membahas pembentukan sistem penarikan pasar wajib untuk perusahaan yang melanggar hukum dan perwalian. Perusahaan-perusahaan ini tidak memenuhi kewajiban laporan tahunan, tidak memiliki informasi kontak yang cukup, tidak melakukan kegiatan produksi dan bisnis dalam jangka waktu yang lama, dan secara serius melanggar hak dan kepentingan konsumen. Ketiga, membangun strategi yang paling efektif untuk kelangsungan hidup dalam jangka panjang. Kami akan menghilangkan perlindungan lokal, intervensi administratif, dan berbagai subsidi ilegal; kami akan menciptakan

mekanisme keluar yang lazim untuk perusahaan yang kurang beruntung melalui persaingan pasar; dan kami akan mengurangi risiko di pasar industri dan regional.

- menciptakan persaingan pasar yang teratur dan adil. Kami akan meningkatkan regulasi, meningkatkan pengawasan yang sedang berjalan dan pasca operasional, menstandarisasi kegiatan produksi dan operasional perusahaan, menjaga persaingan yang sehat, mempertahankan ketertiban, memperkuat keamanan operasi pasar, dan menciptakan lingkungan yang lebih baik untuk pertumbuhan dan operasi entitas pasar.

Kami akan mempertahankan pasar domestik yang terintegrasi. Pertama, kami akan meningkatkan sesuai dengan hukum yang mengatur pertumbuhan ekonomi pasar. Regulasi pasar dan layanan, mendorong bisnis untuk beroperasi secara mandiri dan bersaing secara adil, mendorong konsumen untuk memilih dan mengkonsumsi secara bebas, dan komponen barang dan produksi mengalir secara bebas dan bertukar dengan pijakan yang sama, dapat mempercepat pembentukan pasar nasional yang bersatu dengan pasar yang bersatu, pasar yang terbuka, dan persaingan yang teratur. Kedua, menghapus hambatan yang menghalangi pasar terpadu. Sesuai dengan persyaratan untuk membangun pasar terpadu nasional, menghapus persaingan yang sehat dan pasar terpadu, menghilangkan kebijakan subsidi yang tidak masuk akal untuk industri tertentu, menghentikan monopoli industri dan hambatan pasar, dan memastikan bahwa faktor produksi di semua pasar utama digunakan dengan setara, memastikan bahwa semua orang dapat berpartisipasi dengan adil dalam persaingan. Ketiga, kami akan memperkuat aturan peraturan pasar terpadu. Kami bermaksud untuk meningkatkan penegakan hukum, pengawasan pasar, dan aturan pasar secara bersamaan, dan untuk membuat pengawasan pasar lebih transparan dan transnasional. Peraturan industri dan regional tidak boleh memecah pasar nasional atau membatasi pertumbuhannya. Keempat, kami akan mendukung pasar yang kooperatif dan terbuka.

Di beberapa area utama, kami akan meningkatkan pengawasan pasar. Pertama, kami akan meningkatkan pengawasan pasar melalui internet. Kita harus memprioritaskan regulasi dan inovasi, meningkatkan sistem peraturan pasar online, dan mendorong pertumbuhan yang sehat. mengawasi aktivitas ilegal seperti penjualan palsu di internet, publisitas palsu, promosi palsu, menghilangkan spekulasi satu huruf, fitnah jahat, dan sebagainya, dan memurnikan pasar jaringan. Model baru seperti e-commerce sosial dan mal perangkat lunak seluler, serta bentuk bisnis baru seperti e-commerce pedesaan, e-commerce lintas batas, dan e-commerce layanan, akan kami awasi dengan ketat. memfasilitasi standarisasi perilaku operator komoditas dan layanan online, meningkatkan

respons platform perdagangan online, mendorong sistem otentikasi identitas dan nama asli toko online, dan menjamin standarisasi dan ketertelusuran aktivitas bisnis online. Kami akan meningkatkan sistem pertemuan antar kementerian untuk pengawasan pasar online dan mengembangkan metode baru untuk pengawasan pasar online. Kami akan mendorong pengawasan yang terintegrasi baik secara online maupun offline, dan kami akan mempelajari metode untuk mengawasi risiko, pemeriksaan langsung secara online, penelusuran sumber, investigasi lokal, manajemen kredit, dan pengawasan kualitas produk e-commerce. Kami juga akan meningkatkan basis data operator online dan mendorong pelanggan untuk melakukan pengawasan dan evaluasi online. memperbarui peraturan perundang-undangan dengan cepat, meningkatkan analisis tren pasar online, dan mengurangi risiko transaksi online. Kedua, untuk menghentikan penyebaran skema piramida jaringan, memperkuat investigasi dan hukuman terkait skema piramida jaringan. Untuk meningkatkan risiko, lakukan lebih banyak penelitian dan evaluasi skema piramida baru dengan nama "bisnis Wechat", "e-commerce", dan "investasi konsumsi" di bawah kondisi baru. Peringatan dan pencegahan, dan meningkatkan kapasitas masyarakat untuk menemukan dan menghentikan skema piramida. Ketiga, ketat mengawasi periklanan di Internet dan menghukum periklanan yang salah dan ilegal. Kami akan meningkatkan metode pengawasan periklanan, meningkatkan sistem pemantauan periklanan, dan meningkatkan platform pengawasan periklanan dan pemantauan periklanan Internet. Keempat, kami akan menetapkan standar manajemen di bidang yang terkait. Kami akan memantau tindakan bisnis perusahaan di pasar perdagangan komoditas, meningkatkan sistem disiplin diri, meningkatkan operasi pasar kredit, dan secara aktif mendukung pengembangan sistem kredit pasar. meningkatkan pengawasan kontrak, standarisasi perilaku pengisian layanan, dan pengawasan dan pengawasan agen layanan perantara. Kedua, kami akan meningkatkan pengawasan pasar internet, ekonomi berbagi, dan pasar teknologi tinggi, serta menghentikan penyalahgunaan hak kekayaan intelektual untuk mencegah persaingan dan menghambat inovasi. Keempat, menghentikan tindakan yang melanggar hukum dalam pembuatan dan penjualan barang palsu dan tidak berkualitas. Ketiga, meningkatkan pengawasan terhadap penggunaan Internet untuk mencegah penjualan barang palsu dan barang jelek serta penyebaran informasi ilegal tentang pembuatan dan penjualan barang palsu. Kami akan membangun sistem tanggung jawab yang jelas dan dapat dilacak, memperkuat pengawasan sumber produk palsu dan jelek, membangun mekanisme pengawasan untuk seluruh rantai produksi, peredaran, dan penjualan barang, dan meningkatkan sistem ketertelusuran untuk produk utama.

Menggalakkan pengawasan kualitas. Berkonsentrasi pada strategi untuk meningkatkan Kualitas, kami akan meningkatkan sistem pengukuran nasional, mempercepat integrasi standar kualitas dan keselamatan dengan standar internasional, berfungsi sebagai standar utama, sertifikasi, akreditasi, inspeksi, dan pengujian untuk memberikan kepercayaan, dan meningkatkan kualitas produk dan layanan ke tingkat internasional yang unggul. Meningkatkan inovasi, mengatasi teknologi penting, meningkatkan kecepatan identifikasi cerdas, dan melakukan analisis kuantitatif dan kualitatif. meningkatkan kemampuan pengawasan pasar untuk layanan inspeksi dan pengujian sertifikasi dan akreditasi, dan mendorong adopsinya di bidang yang sedang berkembang seperti e-commerce dan bisnis Wechat. Meningkatkan manajemen layanan dan sistem promosi, dan mendorong tanda komitmen sistem manajemen dan layanan berkualitas.

Implementasi strategi merek dan merek dagang. Pertama, mendorong pertumbuhan merek komoditas. Dengan menerapkan strategi merek dagang, Anda dapat meningkatkan nilai merek dan pengaruh produk. Tingkatkan sistem layanan merek dagang, mekanisme peninjauan, dan promosi seluruh proses pendaftaran merek dagang. Kedua, melindungi hak kekayaan intelektual merek dagang dengan lebih baik. Menindaklanjuti pelanggaran hak kekayaan intelektual, hak dan kepentingan sah perusahaan, dan perlindungan niat baik merek. Kami akan menambah kekuatan. Penyelidikan tentang perlindungan kekayaan intelektual, undang-undang layanan cloud, e-commerce, dan data besar, serta bidang lain. Kami akan meningkatkan pengawasan kredit merek dagang, termasuk pelanggaran yang disengaja atas hak merek dagang, pemalsuan merek dagang, dan tindakan agensi merek dagang ilegal. Kami juga akan meningkatkan hukuman untuk pelanggaran kepercayaan. Ini juga akan mencakup platform berbagi informasi kredit nasional dan sistem pengungkapan informasi kredit perusahaan nasional.

- Menciptakan lingkungan yang aman dan terjamin untuk konsumen pasar. Kami akan membuat sistem untuk mengawasi kualitas komoditas sepanjang proses dari produksi, peredaran, dan konsumsi, dan melindungi hak konsumen. Kami akan meningkatkan pengawasan pasar di sektor-sektor yang melibatkan pelanggan baru. Pertama dan terpenting, kita harus memahami tren yang mendorong peningkatan konsumsi masyarakat. Kita harus memperhatikan area konsumsi baru, model konsumsi baru, dan hotspot konsumsi baru. Kita harus memperhatikan hubungan dan risiko utama. Kita juga harus mengubah cara regulasi dipikirkan dan diterapkan. Kita juga harus meningkatkan pengawasan pasar yang lebih cerdas, menghilangkan potensi risiko konsumsi, dan mendorong pertumbuhan pasar konsumen yang sehat. Kedua, kami akan meningkatkan

perlindungan hak konsumen baru. Spesifikasi untuk listrik, bisnis Wechat, dan area konsumen baru lainnya; memperkuat platform bisnis listrik dan platform sosial; tanggung jawab hukum mesin pencari; penggunaan pemalsuan Internet dan pemalsuan propaganda yang melanggar hak dan kepentingan konsumen; dan memurnikan pasar komoditas jaringan, telepon, telekomunikasi, dan barang penjualan melalui pos tujuh hari tanpa alasan untuk mengembalikan sistem. Kami akan meningkatkan hukuman bagi orang yang menjual, memberikan, atau memperoleh data pribadi pelanggan. Kami akan memperkuat perlindungan data pelanggan. Ketiga, kami akan melakukan pengawasan yang lebih ketat pada segmen konsumen baru. Kami akan menciptakan cara baru untuk mengawasi bisnis baru seperti transportasi online dan berbagi tempat tinggal, meningkatkan standar layanan dan standar, dan membangun sistem regulasi yang mendorong pembangunan dengan standar yang baik.

Kami akan memperkuat sistem yang melindungi hak-hak konsumen. Pertama, memperkuat hak-hak konsumen, meningkatkan tanggung jawab utama perusahaan, meningkatkan biaya pelanggaran ilegal perusahaan, dan meningkatkan efektivitas perlindungan hak-hak masyarakat. Kedua, perbaiki sarana yang tersedia untuk pengaduan dan laporan konsumen. Untuk memenuhi persyaratan untuk memfasilitasi pengaduan konsumen, platform Internet terpadu nasional untuk pengaduan dan laporan konsumen telah dibuat. Platform ini telah dioptimalkan untuk fungsi pengaduan dan laporan di bidang-bidang utama seperti makanan dan obat-obatan, kualitas dan keamanan, dan pengaduan harga. Selain itu, sistem publisitas publik telah dibuat untuk mempromosikan pengaduan konsumen dan melindungi hak-hak mereka. Ketiga, kami akan meningkatkan metode penyelesaian perselisihan konsumsi. Kami akan merencanakan untuk membangun sistem penyelesaian sengketa konsumen yang lebih luas, menyederhanakan proses perselisihan konsumen, dan meningkatkan efektivitas perlindungan. Hak-hak pelanggan menganjurkan operator untuk membuat mekanisme penyelesaian yang cepat untuk masalah konsumsi kecil, dan mendorong mereka untuk mengambil inisiatif untuk bernegosiasi dengan konsumen tentang cara menyelesaikan masalah. Kami akan meningkatkan sistem kompensasi hukuman di sektor konsumen, secara signifikan meningkatkan kompensasi atas pelanggaran hak dan kepentingan konsumen, dan memperkuat mekanisme pengawasan sosial dengan konsumen sebagai pusat, sehingga konsumen dapat menjadi pengawas yang kuat dan pembela tatanan konsumsi. Keempat, kami akan memprioritaskan pembangunan sistem yang melindungi hak-hak konsumen. Kami akan meningkatkan pengembangan peraturan yang mendukung Undang-Undang Perlindungan Hak dan

Kepentingan Konsumen, yang akan meningkatkan keamanan konsumen, integritas operator, dan kepuasan konsumen. Kami akan mempercepat pembentukan mekanisme kerja sama lintas industri dan lintas bidang untuk pengawasan dan penegakan hukum dalam menangani sengketa konsumsi. Kelima, meningkatkan tanggung jawab utama operator bisnis dan produksi. Menetapkan sistem tanggung jawab "siapa yang memproduksi bertanggung jawab, siapa yang menjual bertanggung jawab" meningkatkan biaya perusahaan ilegal dan memperjelas rantai tanggung jawab konsumen. Meningkatkan tanggung jawab untuk jaminan kualitas produk dan mengambil tindakan seperti perbaikan, penggantian, pengembalian, dan kompensasi kerusakan untuk produk yang bermasalah. Kami akan menerapkan standar penetapan harga yang ketat untuk produsen dan operator bisnis, dan kami akan menerapkan sistem harga yang jelas dan publik. Kami akan menerapkan sistem kompensasi di muka untuk sengketa konsumsi dan membangun sistem deposit kualitas barang dan jasa. mengizinkan asosiasi konsumen dan kelompok lain untuk melindungi hak dan kepentingan konsumen.

5. Mekanisme pengawasan pasar

Pertama, penerapan kebijakan persaingan usaha. Sistem kebijakan yang sangat penting untuk mendorong pertumbuhan dan kemakmuran ekonomi pasar berfungsi untuk mengatur tatanan pasar, menjaga persaingan usaha yang sehat, mendorong inovasi, mendorong reformasi kelembagaan, dan meningkatkan efisiensi pasar dan keuntungan sosial. Pertama, mengubah dasar kebijakan persaingan usaha. Memperbaiki sistem kebijakan dan hukum persaingan usaha, memperjelas tujuan prioritas persaingan usaha, membuat mekanisme koordinasi kebijakan, dan mendorong pelaksanaan kebijakan yang efektif. Kedua, kami akan memperbaiki sistem tinjauan usaha yang adil. Salah satu tanggung jawab penting dalam penerapan kebijakan persaingan usaha adalah standarisasi dan pembatasan tindakan pemerintah. Kami akan menerapkan dan meningkatkan sistem tinjauan persaingan usaha yang sehat, mempelajari dan merumuskan aturan rinci untuk pelaksanaan tinjauan persaingan usaha yang sehat, membantu organ pembuat kebijakan dalam melaksanakan tinjauan persaingan usaha yang sehat, membersihkan kebijakan dan aturan yang relevan, dan memastikan bahwa kebijakan dan aturan yang relevan diterapkan.

Kedua, kami akan meningkatkan sistem pengawasan kredit perusahaan. Kami akan meningkatkan sistem pengawasan kredit perusahaan, meningkatkan rasa tanggung jawab perusahaan, meningkatkan mekanisme pengendalian diri perusahaan, membiarkan kredit menciptakan kekayaan, mengakumulasi kekayaan dengan kredit, memberikan peran penuh pada peran penting kredit dalam operasi ekonomi, dan mendorong pembangunan sistem kredit

sosial. Pertama, kami akan meningkatkan sistem pengungkapan informasi perusahaan; meningkatkan sistem pengungkapan informasi perusahaan; meningkatkan keamanan transaksi antar perusahaan; mengurangi risiko transaksi pasar; dan meningkatkan efisiensi ekonomi. Kami juga akan meningkatkan transparansi dan keterbukaan pengawasan pasar dan hukum administratif; dan mempublikasikan informasi tentang hukuman administratif. Kami akan mendukung penggunaan media baru dan sumber lain untuk menyebarkan informasi tentang kredit entitas pasar serta menyediakan metode yang mudah dan efektif bagi masyarakat untuk meminta informasi. Kedua, memperkuat mekanisme pengumpulan informasi perusahaan. Pengumpulan informasi perusahaan merupakan dasar untuk pengawasan kredit, pengawasan kolaboratif, hukuman bersama, dan tata kelola sosial bersama. Memperkuat integrasi informasi, menciptakan metode untuk mengumpulkan informasi terkait kredit perusahaan, menggabungkan sumber daya informasi yang terkait dengan perusahaan dari berbagai departemen, dan memecahkan masalah informasi perusahaan yang terfragmentasi, terdesentralisasi, dan terregionalisasi. Dengan menggunakan sistem publisitas informasi kredit perusahaan nasional, informasi dasar tentang perusahaan, lisensi dan hukuman administratif, serta informasi peraturan lainnya yang dibuat oleh departemen pemerintah dalam tindakan mereka, dikumpulkan untuk kepentingan perusahaan. Ini memberikan gambaran yang indah tentang perusahaan dari berbagai perspektif. membuat mekanisme untuk pertukaran informasi antara departemen, menggunakan platform berbagi informasi kredit nasional dan sistem publisitas informasi kredit perusahaan nasional, mendorong pemerintah dan departemen terkait untuk berbagi informasi dengan cepat dan efektif, dan memecahkan "pulau" informasi. Ketiga, kami akan meningkatkan sistem hukuman bersama untuk pelanggaran kepercayaan dan pengekangan kredit. memberikan perhatian penuh pada tugas pengawasan kredit perusahaan dan mendukung operasi bisnis yang transparan. Kami akan memperbaiki daftar operasi yang tidak masuk akal dan daftar perusahaan yang sangat ilegal dan melanggar kepercayaan, dan kami akan menggunakan informasi kredit sebagai dasar penting untuk menghukum entitas pasar yang melanggar kepercayaan. Kami akan melakukan hukuman kredit antar departemen dan meningkatkan hukuman bagi perusahaan yang melanggar kep Kami akan menerapkan manajemen rahasia risiko kredit untuk bisnis, memberikan kiat risiko sesuai dengan catatan kredit bisnis, dan meningkatkan pengawasan rahasia dan pencegahan risiko. Menciptakan prosedur untuk memperbaiki kredit bisnis untuk mendorong bisnis untuk memperbaiki kredit mereka.

Ketiga, memperkuat pengawasan big data. Kami akan mendorong modernisasi pengawasan pasar dengan informatisasi pengawasan pasar, memanfaatkan data besar dan teknologi

informasi generasi berikutnya, meningkatkan kemampuan untuk menggunakan data besar, mewujudkan inovasi regulasi melalui "Internet +", menurunkan biaya regulasi, meningkatkan efisiensi regulasi, dan meningkatkan kebijaksanaan dan ketepatan pengawasan pasar. Pertama, kami akan meningkatkan pemanfaatan big data secara keseluruhan. Kami akan meningkatkan analisis data besar secara menyeluruh, mengintegrasikan pendaftaran industri dan komersial, mengawasi kualitas dan keamanan, keamanan pangan, penegakan hukum persaingan usaha, perlindungan hak konsumen, sumber daya data perusahaan dan perusahaan, melakukan penelitian untuk membangun model regulasi data besar, meningkatkan pemantauan dan analisis lingkungan pasar, prediksi dan peringatan dini, dan meningkatkan kualitas produk dan layanan. Selanjutnya, kami akan meningkatkan pembangunan infrastruktur big data. Mempromosikan pembangunan informatisasi "Internet+ super-visi" dan meningkatkan tingkat informatisasi pengawasan kredit pemerintah untuk menyesuaikan diri dengan tren pengawasan data besar. Mengembangkan sistem standar big data dan mempelajari dan mengembangkan standar dasar, teknis, aplikasi, dan manajemen yang terkait dengan big data. Kami juga akan membantu mempercepat penetapan standar teknis untuk pengumpulan, penyimpanan, pengungkapan, pengungkapan, pembagian, penggunaan, jaminan kualitas, dan manajemen keamanan informasi pemerintah. Kami juga akan membantu menetapkan standar dan norma untuk berbagi dan pertukaran data antara bisnis. Untuk menjaga keamanan data nasional, serta data warga negara, badan hukum, dan organisasi lainnya, kami akan membangun sistem jaminan keamanan data yang kuat. Ketiga, kami akan mengeksplorasi industri layanan kredit yang berbasis data besar. Kami akan secara aktif namun hati-hati mendukung penyebaran data peraturan pasar kepada masyarakat, memperjelas wewenang dan ruang lingkup pemerintah untuk memanfaatkan data besar entitas pasar, dan membangun mekanisme penggunaan data untuk komunikasi antara pemerintah dan masyarakat. Kami akan meningkatkan kolaborasi dengan bisnis dan lembaga sosial, dan bergantung pada perusahaan profesional untuk menerapkan data pengawasan pasar yang signifikan melalui pengadaan pemerintah, outsourcing layanan, dan urun daya sosial, antara metode lainnya, untuk mengurangi biaya pengawasan pasar. mengembangkan berbagai jenis layanan kredit; mendorong agen pelaporan kredit, asosiasi konsumen, bisnis online, organisasi industri, dan kekuatan sosial lainnya untuk mengumpulkan informasi kredit perusahaan sesuai dengan hukum; membangun mencakup berbagai bidang, setiap tautan ke catatan kredit badan utama pasar; menyediakan lebih banyak produk dan layanan kredit; dan memperluas laporan kredit di bidang pengawasan pasar dan layanan publik. Terbukanya informasi pemerintah, data, dan sumber daya informasi sosial harus meningkatkan transparansi kegiatan produksi dan operasi entitas pasar. Selain itu, media

berita, organisasi industri, pemangku kepentingan, dan konsumen harus memiliki kesempatan untuk berpartisipasi dalam pengawasan entitas pasar.

6. Sistem pengawasan pasar

Untuk memperkuat serta meningkatkan visi strategis pasar modern, langkah-langkah akan diambil guna menyelaraskan sistem pengawasan pasar, mengoptimalkan pemanfaatan sumber daya penegakan hukum, menyatukan regulasi, dan membangun mekanisme pengawasan yang lebih efisien serta terkoordinasi. Dengan pendekatan ini, diharapkan terbentuk sistem pengawasan yang lebih luas, terstruktur, dan berorientasi pada layanan.

Penegakan hukum yang komprehensif menjadi aspek krusial dalam pengawasan pasar dan perlu didorong secara maksimal. Dengan berpegang pada prinsip keseragaman dalam pasar dan regulasi hukum, akan dilakukan evaluasi menyeluruh terkait cakupan serta metode reformasi yang paling efektif. Standarisasi dalam kualifikasi serta prosedur penegakan hukum juga akan diperkuat guna meningkatkan efisiensi serta efektivitas dalam implementasi regulasi di lapangan.

Kolaborasi antara berbagai departemen akan ditingkatkan dengan memperjelas peran pengawasan masing-masing sektor, baik secara menyeluruh maupun berdasarkan industri tertentu. Dibentuknya mekanisme kerja sama yang lebih sinergis antara regulator utama dan otoritas industri bertujuan untuk menciptakan sistem pengawasan yang lebih terstruktur, dengan komunikasi yang efektif serta pembagian tugas yang jelas. Mengacu pada prinsip "yang menyetujui bertanggung jawab, yang mengawasi harus menindak," sistem regulasi akan terus disempurnakan agar dapat menjaga persaingan pasar yang sehat, melindungi hak konsumen, serta mendukung pertumbuhan ekonomi berbasis pasar.

Sejalan dengan konsep tata kelola modern, upaya akan difokuskan pada pembentukan mekanisme pengawasan pasar yang melibatkan berbagai pihak, termasuk pemerintah, industri, dan masyarakat. Legislasi terkait tata kelola berbasis partisipasi sosial akan diprioritaskan guna memperjelas hak serta tanggung jawab masing-masing pihak dalam pengawasan pasar. Selain itu, pengawasan publik, peran media, serta keterlibatan konsumen akan ditingkatkan sebagai bagian dari sistem yang lebih transparan. Dengan demikian, sistem pengawasan pasar yang lebih menyeluruh dapat diwujudkan, menciptakan ekosistem bisnis yang sehat dan berkelanjutan.

6.3.4 Disiplin Diri Industri dan Pengawasan Sosial

1. Pentingnya disiplin diri industri dan pengawasan social

Salah satu langkah penting dalam pengendalian risiko transaksi e-commerce adalah disiplin diri industri dan pengawasan sosial. UU E-commerce mendefinisikan peran penting dari kedua disiplin ini, menekankan pentingnya pembentukan sistem manajemen kolaboratif yang sesuai dengan karakteristik e-commerce, dan mendorong pembentukan sistem tata kelola pasar e-commerce dengan partisipasi bersama dari departemen terkait, organisasi industri e-commerce, operator e-commerce, dan organisasi masyarakat.

2. Disiplin diri industry

Pengendalian diri industri juga dikenal sebagai disiplin diri industri. Ini terdiri dari dua bagian: kepatuhan industri terhadap hukum, peraturan, dan kebijakan nasional, serta penerapan aturan dan kontrak industri untuk membatasi perilaku mereka sendiri; keduanya juga mencakup fungsi pengawasan dan perlindungan anggota industri. Tujuan dari disiplin diri industri adalah untuk mengatur perilaku industri, mengkoordinasikan kepentingan rekan-rekan, menjaga keamanan, dan meningkatkan efisiensi.

Dalam beberapa kasus, perilaku anggota industri dibatasi oleh disiplin diri industri. Di satu sisi, peraturan nasional berlaku. Pada tahun 2017, Dewan Negara mengeluarkan "pilihan yang jauh lebih mencolok - dan konsekuensi yang lebih berat - dalam" perencanaan regulasi pasar, menunjukkan bahwa reformasi organisasi industri memperkuat fungsi otonomi organisasi industri, mendorong partisipasi dalam standar industri dan spesifikasi disiplin diri industri, membangun sistem kredit industri, memberikan peran penuh untuk pengembangan perusahaan jasa, dan membakukan perilaku badan utama industri. Menurut Pasal 6 dari Langkah-langkah untuk Pengawasan dan Administrasi Perdagangan Online, departemen pengawasan dan administrasi pasar harus mengarahkan operator komoditas jaringan, organisasi industri perdagangan online, organisasi konsumen, dan konsumen untuk berpartisipasi dalam tata kelola pasar perdagangan online. Mereka juga harus mendorong peningkatan partisipasi yang beragam, koordinasi yang efektif, dan sistem tata kelola pasar perdagangan online yang terstandardisasi dan dapat diandalkan. Pasal 8 Undang-Undang Perdagangan Elektronik Republik Rakyat Tiongkok menetapkan bahwa organisasi industri terkait jaringan harus memperkuat disiplin diri industri, sistem, dan norma perilaku keamanan jaringan, memandu anggota untuk meningkatkan perlindungan keamanan jaringan, meningkatkan tingkat perlindungan jaringan, dan mendorong pertumbuhan industri yang sehat. Pasal 11 Undang-Undang Keamanan Siber Republik Rakyat Tiongkok menetapkan bahwa organisasi industri terkait jaringan harus bekerja sama dengan asosiasi. Sisi lain dari peraturan industri. Anggota

industri berkolaborasi untuk membuat konvensi. Selain itu, konvensi disiplin diri industri juga merupakan kontrak yang disepakati oleh setiap anggota melalui perundingan. memiliki konsekuensi yang sama dengan hukum. Konvensi industri memastikan kemajuan yang lancar dalam pengaturan industri mandiri karena berfungsi sebagai aturan dasar untuk pelaksanaan hak dan kewajiban anggota industri.

Industri yang berdisiplin diri harus memiliki organisasi manajemen yang sesuai untuk mengelola dan mengawasi. Didasarkan pada asosiasi industri, organisasi manajemen disiplin diri industri dikenal sebagai organisasi industri. Organisasi industri yang efektif sangat penting untuk keberhasilan industri disiplin diri. Karena itu, perusahaan e-commerce harus mendisiplinkan diri, meningkatkan standar industri, membangun sistem kredit, membantu operator berpartisipasi dalam persaingan pasar secara legal dan adil melalui mekanisme kerja sama dan keterkaitan, dan bekerja sama dengan lembaga administratif untuk mengawasi dan mengawasi industri.

3. Pengawasan social

Untuk mencegah dan mengatasi risiko keamanan transaksi e-commerce, perlu dilakukan pengawasan yang beragam; partisipasi konsumen merupakan bagian penting dari pengawasan yang beragam ini.

Pertama, berikan organisasi konsumen peran penuh dalam menjaga hak dan kepentingan konsumen. Organisasi seperti asosiasi konsumen dan organisasi lain harus memiliki peran penuh dalam hal ini. Kami akan mendorong untuk memperluas cakupan subjek litigasi kepentingan publik, meningkatkan jenis litigasi, dan meningkatkan litigasi kepentingan publik untuk industri monopoli, utilitas publik, bidang-bidang yang sedang berkembang, dan peristiwa penting yang berkaitan dengan kepentingan konsumsi masyarakat. Uji coba dan survei pengalaman akan dilakukan dan laporan survei otoritatif akan dirilis secara tepat waktu untuk meningkatkan kemampuan konsumen untuk melindungi diri sendiri. Berpartisipasi aktif dalam legislatif dan standar yang berkaitan dengan hak dan kepentingan konsumen. Kami akan meningkatkan pembangunan asosiasi konsumen di tingkat komunitas dan memastikan bahwa asosiasi konsumen melakukan apa yang harus mereka lakukan. Kami akan memberikan akses penuh ke komite ahli, asosiasi konsumen, dan sukarelawan perlindungan hak-hak konsumen, memberikan konsultasi konsumen profesional, meningkatkan layanan hukum, dan melindungi kelompok rentan. Kami akan meningkatkan pendidikan dan pedoman tentang konsumsi, memberikan pedoman untuk konsumsi, memberikan peringatan risiko, dan mendorong konsumsi yang rasional dan logis. Kedua, mendorong pelanggan untuk melakukan pengawasan dan evaluasi jaringan. Membantu mereka memahami bidang konsumsi jaringan yang terkait

dengan harga kehidupan konsumen, periklanan, penyelesaian sengketa, sikap layanan, perlindungan informasi pribadi konsumen, dan masalah lainnya, dan mendorong departemen terkait untuk mengambil tindakan untuk mengendalikan perilaku bising. Selain itu, kami akan meningkatkan mekanisme perlindungan hak dan kepentingan konsumen. Kami harus secara aktif mengeksplorasi sistem dan langkah-langkah perlindungan hak dan kepentingan konsumen yang efektif di internet. Kami harus bekerja sama dengan operator e-commerce untuk membangun mekanisme penghubung kerja perlindungan hak dan kepentingan konsumen, membantu operator situs web kelompok pengawasan untuk membangun dan meningkatkan sistem perlindungan hak dan kepentingan konsumen, dan memastikan bahwa situs web operasi e-commerce memiliki sistem perlindungan hak dan kepenting Pada saat yang sama, semua daerah harus secara aktif memberikan pendidikan konsumen secara online dan secara teratur mempublikasikan kasus dan perilaku ilegal kepada masyarakat melalui informasi peringatan dan bentuk lainnya. Tujuan dari ini adalah untuk meningkatkan kesadaran konsumen dan membantu mereka melindungi hak dan kepentingan mereka yang sah dari risiko.

BAB 7
Mengendalikan Risiko Kredit dalam E-commerce

Nilai-nilai dasar bisnis adalah kejujuran dan kepercayaan. Sampai batas tertentu, ekonomi pasar adalah ekonomi kredit dalam ekonomi komoditas maju saat ini karena kredit dan pasar saling terkait erat. Kredit yang terbatas hanya dapat menciptakan pasar yang terbatas, pasar tanpa kredit hanya dapat menjadi pasar yang tidak lengkap. Dalam kegiatan ekonomi, orang atau organisasi perlu mengembangkan kepercayaan, pertama adalah menjaga kepercayaan, kedua adalah memiliki kapasitas untuk menjaga kepercayaan. Di antara keduanya, menjaga kepercayaan adalah persyaratan yang diperlukan untuk mendapatkan kepercayaan, tanpa itu, seseorang tidak dapat mengembangkan kepercayaan. Kapasitas untuk menjaga kepercayaan adalah sarana teknologi dan keuangan untuk memenuhi janji kita. Kedua komponen ini tidak hanya memenuhi standar perilaku moral tetapi juga memiliki hubungan yang erat dengan keterbatasan institusional. Dalam bisnis e-commerce tanpa tatap muka, hal ini sangat penting. Jika sistem kredit, kebijakan perusahaan, dan iklim bisnis gagal, pemutusan hubungan kepercayaan akan menjadi sangat umum dan menimbulkan risiko signifikan yang membahayakan pertumbuhan e-commerce secara berkelanjutan.

7.1 Identifikasi Risiko Kredit E-commerce

Identifikasi risiko kredit dalam e-commerce berarti mengidentifikasi risiko kredit atau perilaku yang melanggar kepercayaan yang ada dalam industri e-commerce. Untuk menemukan risiko kredit, pertama-tama kita harus mempelajari definisi kredit dan risiko kredit. Kemudian, kita harus mempelajari faktor-faktor yang mempengaruhi dan mengapa risiko kredit muncul, dan terakhir, kita harus menjelaskan bagaimana risiko kredit berfungsi.

7.1.1 Konsep Terkait Risiko Kredit E-commerce

1. Konsep Kredit E-Commerce

Pertama, kredit. Kredit dapat dikategorikan menjadi kredit kepribadian dan kredit sistem. Kredit kepribadian berakar pada hubungan sosial tertentu, yakni kredit yang bersifat personal dan terbentuk melalui interaksi interpersonal yang didasarkan pada kepercayaan. Dalam sistem sosial, struktur tata kelola yang diterapkan adalah model "berbasis hubungan". Sementara itu, kredit sistem mengacu pada kepercayaan terhadap sistem yang melibatkan individu-individu yang tidak saling mengenal. Hubungan kredit ini dibangun melalui kontrak, hukum, serta regulasi, di mana kekuatan mengikat dari aturan-aturan tersebut berfungsi sebagai jaminan. Dalam sistem sosial, pendekatan yang digunakan adalah struktur aturan hukum yang "berbasis sistem hukum". Kepercayaan kepribadian bergantung pada keterikatan emosional dan norma

moral, tetapi seiring dengan semakin luasnya jangkauan individu dan transaksi, biaya untuk identifikasi serta pengawasan pun meningkat drastis. Sebaliknya, kepercayaan sistem menawarkan hubungan kredit yang lebih stabil dan berjangka panjang. Kredit yang disebutkan selanjutnya mengacu pada jenis kredit ini.

Kredit berkaitan erat dengan tingkat kepercayaan yang diperoleh seseorang atau entitas dalam memenuhi suatu komitmen. Oleh karena itu, sebelum membahas kredit lebih lanjut, perlu dipahami terlebih dahulu konsep komitmen. Berdasarkan cara seseorang atau suatu pihak membuat komitmen, komitmen dapat diklasifikasikan menjadi dua jenis utama: komitmen tersurat dan komitmen tersirat. Komitmen tersurat merupakan pernyataan janji yang disampaikan secara eksplisit melalui kata-kata, baik secara lisan maupun tertulis. Komitmen tertulis sendiri terbagi menjadi dua bentuk, yaitu komitmen dalam dokumen fisik dan komitmen dalam format elektronik. Dalam konteks e-commerce, komitmen pada umumnya termasuk dalam kategori komitmen tertulis. Selain itu, janji yang dibuat oleh para pihak dalam transaksi e-commerce serta komitmen yang mengikuti standar industri juga tergolong dalam bentuk komitmen tertulis. Sementara itu, komitmen tersirat merujuk pada janji yang tidak secara eksplisit dinyatakan, tetapi tercermin dalam tindakan atau kepatuhan terhadap norma yang berlaku. Sebagai contoh, kepatuhan terhadap hukum nasional dapat dianggap sebagai bentuk komitmen tersirat, begitu pula praktik bisnis yang jujur mencerminkan komitmen tersirat pelaku e-commerce terhadap etika bisnis dan moralitas publik. Pada dasarnya, kredit memiliki keterkaitan yang erat dengan aspek moral dan hukum. Dengan kata lain, kredit bukan hanya sekadar persoalan hukum, tetapi juga merupakan permasalahan moral. Dalam dunia e-commerce, penilaian terhadap tingkat kredit suatu pihak didasarkan pada dua faktor utama: pertama, adanya regulasi, standar, dan perjanjian yang telah disepakati secara jelas oleh para pihak yang terlibat, dan kedua, kepatuhan terhadap etika bisnis serta moralitas publik yang tidak selalu tertulis. Jika kedua aspek ini dilanggar, maka risiko kredit akan meningkat, yang pada akhirnya dapat berdampak negatif pada reputasi dan kepercayaan dalam dunia bisnis.

Selanjutnya, kredit e-commerce. Kredit e-commerce merujuk pada kemampuan seorang pedagang dalam membangun dan mempertahankan kepercayaan dari pihak lain sebagai dasar dalam transaksi daring. Kepercayaan ini diperoleh melalui praktik bisnis yang jujur, kepatuhan terhadap komitmen serta perjanjian transaksi, dan upaya memenuhi ekspektasi wajar dari mitra bisnisnya. Dalam konteks digital, kredit e-commerce merupakan pengembangan dari konsep kredit dalam pasar tradisional yang diadaptasi ke dalam ekosistem perdagangan elektronik. Mengingat bahwa transaksi e-commerce umumnya berlangsung secara daring, tingkat kepercayaan ini sangat bergantung pada faktor-faktor seperti keandalan

serta stabilitas platform perdagangan online yang digunakan. Dengan demikian, semakin baik reputasi dan kredibilitas suatu platform, semakin besar pula kemungkinan para pedagang dan konsumen merasa aman dalam bertransaksi.

2. Risiko Kredit Perdagangan Elektronik

Risiko kredit merujuk pada potensi kerugian yang timbul akibat kegagalan dalam memenuhi kewajiban kredit, yang sering disebut sebagai pelanggaran kepercayaan. Dengan kata lain, risiko ini muncul ketika suatu pihak gagal mempertahankan kepercayaan yang telah diberikan kepadanya. Dalam banyak kasus, pelanggaran kepercayaan menjadi inti dari permasalahan risiko kredit, sehingga studi tentang risiko kredit pada dasarnya juga merupakan kajian tentang faktor-faktor yang menyebabkan hilangnya kepercayaan dalam suatu transaksi. Pelanggaran kepercayaan terjadi ketika seseorang atau entitas bertindak dengan cara yang mengikis kepercayaan pihak lain yang terlibat dalam transaksi. Dalam konteks e-commerce, pihak-pihak yang terdampak oleh pelanggaran ini bisa berupa perusahaan, individu, maupun organisasi lainnya yang berpartisipasi dalam transaksi digital. Dari perspektif hukum dan regulasi, tindakan yang dikategorikan sebagai pelanggaran kepercayaan telah diatur dalam berbagai ketentuan, termasuk undang-undang, peraturan administratif, peraturan departemen, hingga kebijakan daerah. Secara khusus, pelanggaran kepercayaan dapat mencakup wanprestasi (seperti pelanggaran kontrak, ketidaksesuaian terhadap perjanjian transaksi, atau ketidakpatuhan terhadap norma perdagangan), serta tindakan ilegal atau kriminal yang dapat berdampak pada stabilitas dan kepercayaan dalam ekosistem e-commerce.

Selanjutnya Risiko kredit e-commerce. Risiko kredit e-commerce mengacu pada tingkat ketidakpastian mengenai apakah suatu pihak dalam transaksi digital akan mematuhi kontrak pasar serta peraturan yang berlaku. Pada dasarnya, risiko ini berkaitan erat dengan aspek hukum dan moral dalam aktivitas e-commerce. Salah satu konsekuensi utama dari risiko kredit e-commerce adalah kerugian akibat pelanggaran kepercayaan, terutama yang berkaitan dengan ketidakpatuhan terhadap etika bisnis dan nilai-nilai moral dalam masyarakat. Ketika suatu pihak bertindak tidak jujur atau melanggar komitmen yang telah disepakati, dampaknya tidak hanya menghambat perkembangan ekosistem e-commerce yang sehat dan teratur, tetapi juga dapat mengganggu stabilitas hukum serta memperlambat kemajuan dalam membangun norma moral di lingkungan sosial yang lebih luas.

7.1.2 Faktor Dampak dan Asal Mula Risiko Kredit E-commerce

1. Faktor-Faktor Risiko Kredit E-Commerce

Pertama, kesadaran integritas dan etika bisnis. Kejujuran merupakan salah satu prinsip fundamental dalam moralitas kewarganegaraan, pondasi utama bagi pertumbuhan ekonomi berbasis pasar, serta elemen kunci dalam etika bisnis. Kesadaran akan pentingnya kredit mencerminkan nilai-nilai, cara pandang terhadap dunia, serta pemahaman mengenai kepercayaan dari suatu entitas dalam sistem kredit. Hal ini mencakup kualitas dasar dalam menjaga reputasi, tingkat moralitas yang dianut, serta standar etika yang dijunjung tinggi—semuanya menjadi cerminan dari sejauh mana suatu pihak bersedia untuk memenuhi kewajibannya dalam suatu perjanjian. Bagi sebuah perusahaan, kesadaran akan integritas tercermin dalam budaya korporasi yang diterapkan. Prinsip-prinsip moral yang melekat dalam nilai-nilai perusahaan menjadi bagian dari identitas serta budaya kerja yang dikembangkan. Sementara itu, dalam lingkup pasar, kesadaran terhadap integritas dan etika bisnis tergambar melalui berbagai keputusan serta tindakan yang diambil oleh para pelaku usaha. Faktor-faktor ini memiliki pengaruh besar terhadap tingkat kepercayaan dan reputasi kredit yang mereka bangun di mata mitra bisnis serta masyarakat luas.

Selanjutnya, hukuman atas pelanggaran kepercayaan. Tingkat keparahan hukuman terhadap pelanggaran kepercayaan berperan besar dalam menentukan konsekuensi yang harus ditanggung oleh pihak yang melanggar. Semakin tinggi biaya yang harus dikeluarkan akibat pelanggaran kepercayaan, semakin kecil insentif bagi seseorang untuk melakukan tindakan tersebut. Jika potensi kerugian dari melanggar kepercayaan sama besar atau bahkan melebihi keuntungan yang diperoleh dari tindakan tersebut, maka pelaku cenderung menghindari perilaku yang merugikan. Inilah inti dari manajemen risiko kredit—menciptakan sistem yang mampu menekan tindakan pelanggaran dengan memberlakukan sanksi yang efektif.

Terakhir, membangun sistem kredit yang kuat dan komprehensif merupakan langkah krusial dalam mengurangi risiko kredit, khususnya dalam ekosistem e-commerce. Sistem yang tidak terstruktur dengan baik dapat meningkatkan ketidakpastian dalam transaksi digital dan memperbesar risiko kehilangan kepercayaan. Oleh karena itu, pengembangan sistem kredit yang lebih transparan, akurat, dan dapat diandalkan menjadi solusi utama dalam menciptakan lingkungan e-commerce yang aman dan terpercaya.

2. Asal Mula Risiko Kredit E-Commerce

E-commerce beroperasi dalam pasar virtual yang berbasis pada jaringan informasi. Dalam ekosistem ini, perbedaan tingkat kredibilitas serta etika bisnis di antara pelaku transaksi dapat menimbulkan ketidakpastian terkait kepatuhan mereka terhadap kontrak pasar, baik yang

bersifat tersurat maupun tersirat. Ketidakpastian inilah yang pada akhirnya memicu munculnya risiko kredit dalam e-commerce. Secara alami, tindakan yang tidak amanah dilakukan oleh individu yang kurang memiliki integritas. Dalam lingkungan e-commerce, pengelola platform berusaha mengelola kredit dengan memastikan bahwa karyawannya memiliki rekam jejak yang baik. Namun, ada dua jenis individu yang berpotensi menimbulkan risiko: mereka yang secara terbuka tidak memiliki loyalitas, serta mereka yang menyembunyikan ketidakjujuran atau tidak bekerja sama. Tantangan terbesar bagi operator e-commerce adalah kesulitan dalam mendeteksi, menyelidiki, dan mengumpulkan bukti terkait perilaku tidak amanah ini. Untuk mengatasi hambatan tersebut, operator e-commerce sering kali mengandalkan lembaga investigasi kredit pihak ketiga serta departemen pemerintah terkait sebagai sumber utama dalam memperoleh informasi mengenai pelanggaran kepercayaan eksternal. Dengan demikian, mekanisme pengawasan dan pemantauan dari pihak eksternal menjadi faktor penting dalam menjaga kredibilitas dan transparansi dalam ekosistem e-commerce.

7.1.3 Kinerja Risiko Kredit E-commerce

Untuk mencegah risiko kredit dalam e-commerce, langkah awal yang harus dilakukan adalah mengidentifikasi berbagai bentuk perilaku yang melanggar kepercayaan. Tingkat keparahan dari pelanggaran ini secara langsung mencerminkan sejauh mana risiko kredit yang dapat timbul. Salah satu cara untuk mengklasifikasikan pelanggaran ini adalah dengan melihat jenis serta jumlah hukuman administratif yang telah dijatuhkan kepada pihak yang melakukan pelanggaran.

Secara umum, perilaku melanggar kepercayaan dapat dibagi ke dalam dua kategori utama. Kategori pertama mencakup pelanggaran serius yang secara eksplisit telah diatur dalam undang-undang, peraturan administratif, serta regulasi yang ditetapkan oleh otoritas terkait. Pelanggaran dalam kategori ini biasanya memiliki dampak yang signifikan terhadap ekosistem e-commerce dan dapat dikenakan sanksi yang lebih berat.

Sementara itu, kategori kedua mencakup berbagai bentuk pelanggaran terhadap hukum, peraturan administratif, serta kebijakan internal yang berlaku, namun belum mencapai tingkat keparahan sebagaimana yang terdapat dalam kategori pertama. Meskipun dampaknya mungkin tidak sebesar pelanggaran serius, tindakan dalam kategori ini tetap berkontribusi terhadap meningkatnya risiko kredit dan dapat mengurangi tingkat kepercayaan dalam transaksi e-commerce. Oleh karena itu, pengawasan yang ketat serta sistem mitigasi risiko yang efektif menjadi sangat penting untuk menjaga stabilitas dan kepercayaan dalam lingkungan digital.

1. Pelanggaran Kepercayaan yang Serius

Menurut berbagai ketentuan hukum dan kebijakan, kinerja perilaku melanggar kepercayaan yang serius adalah sebagai berikut, dan kinerja perilaku melanggar kepercayaan yang serius ditunjukkan pada **Tabel 7.1**.

Tabel 7.1 Pelanggaran Kepercayaan yang Serius

Perilaku Melanggar Kepercayaan yang Serius	Menurut
1. Tindakan yang secara serius membahayakan kesehatan dan keselamatan jiwa manusia, termasuk perilaku yang melanggar kepercayaan serius dalam hal makanan dan obat-obatan, ekologi lingkungan, kualitas teknik, keselamatan produksi, keselamatan kebakaran, sertifikasi produk wajib, dan bidang lainnya 2. Kerusakan serius pada tatanan persaingan pasar yang adil dan perilaku tatanan sosial yang normal, termasuk penyuapan, penghindaran pajak, utang yang jahat penghindaran, pembayaran gagal bayar atau biaya layanan yang berbahaya, pembayaran kembali yang berbahaya, penggalangan dana ilegal, penipuan kontrak, skema piramida, tidak berlisensi, memproduksi produk palsu dan pelanggaran hak kekayaan intelektual yang disengaja, pinjam meminjam penawaran kualifikasi, sekitar, palsu periklanan, konsumen atau sekuritas dan investor berjangka yang sah, hak dan kepentingan yang sah, kerusakan serius tatanan komunikasi dunia maya, mengganggu ketertiban sosial dan ketidakjujuran serius lainnya 3. Tindakan menolak untuk melakukan kewajiban hukum yang secara serius mempengaruhi kredibilitas organ peradilan dan administrasi, termasuk tindakan serius tindakan melanggar kepercayaan seperti para pihak yang memiliki kemampuan untuk melaksanakan tetapi menolak untuk melaksanakan atau menghindari eksekusi setelah putusan atau keputusan organ yudisial membuat penilaian atau Keputusan	Panduan dari Dewan Negara mengenai Pembentukan dan Peningkatan Sistem untuk Menjaga Kepercayaan serta Penerapan Sanksi Kolektif terhadap Pelanggaran Kepercayaan dalam Rangka Mempercepat Penguatan Integritas Sosial (Guofa [2016] No.33).

Perilaku Melanggar Kepercayaan yang Serius	Menurut
4. Menolak untuk melakukan kewajiban pertahanan negara, menolak atau menghindari dinas militer, menolak atau menunda permintaan sumber daya sipil atau menghambat transformasi sumber daya sipil yang dibutuhkan, membahayakan kepentingan pertahanan nasional dan merusak fasilitas pertahanan nasional	
Ketika pihak yang bersangkutan melanggar hukum atau peraturan administratif, bersifat buruk, memiliki keadaan yang serius, sangat merugikan masyarakat, dan dikenakan hukuman administratif yang berat oleh departemen pengawasan dan administrasi pasar, departemen pengawasan dan administrasi pasar departemen administrasi akan dimasukkan dalam daftar pelanggaran hukum dan pelanggaran kepercayaan yang serius sesuai dengan ketentuan. Tindakan-tindakan ini. , hukuman administratif yang lebih berat termasuk: 1) Denda akan dikenakan sesuai dengan standar kebijaksanaan denda administratif dan sesuai dengan prinsip hukuman yang lebih berat; 2) Mengurangi tingkat kualifikasi, mencabut lisensi dan izin usaha; 3) Membatasi produksi dan aktivitas bisnis, menangguhkan produksi atau bisnis, menutup, atau membatasi pekerjaan; Hukuman administratif lain yang lebih berat seperti yang ditentukan oleh undang-undang, peraturan administratif, dan peraturan departemen Pelanggaran serius dan perilaku yang melanggar kepercayaan meliputi: (1) Tindakan ilegal yang serius di bidang keamanan pangan (2) Perbuatan melawan hukum yang serius di bidang obat, alat kesehatan, dan kosmetik (3) Tindakan ilegal yang serius di bidang kualitas dan keselamatan (4) Tindakan ilegal serius yang melanggar hak dan kepentingan konsumen	Pedoman Pengelolaan Daftar Pelanggaran Serius yang Merusak Kepercayaan dalam Pengawasan dan Regulasi Pasar (Peraturan No. 44, Administrasi Negara untuk Regulasi Pasar, 30 Juli 2021).

Perilaku Melanggar Kepercayaan yang Serius	Menurut
(5) Tindakan ilegal serius yang mengganggu tatanan persaingan usaha yang sehat dan mengganggu tatanan pasar (6) Perbuatan-perbuatan ilegal berikut ini, yang bersifat buruk, dalam keadaan serius dan menyebabkan kerugian sosial yang besar, dan dapat dikenai hukuman berat hukuman administratif oleh departemen pengawasan dan administrasi pasar, akan dimasukkan dalam daftar pelanggaran berat dan merusak kepercayaan: 1) Terlibat dalam kegiatan bisnis tanpa memperoleh izin lain sesuai dengan hukum; 2) Menyerahkan materi palsu atau mengambil cara lain untuk menyembunyikan fakta-fakta penting, memperoleh izin administratif, memperoleh, mengubah, atau membatalkan pendaftaran entitas pasar, atau mengubah, menjual kembali, menyewakan atau menjual lisensi atau izin usaha; Menolak, menghalangi, atau mengganggu departemen pengawasan dan administrasi pasar untuk melakukan pengawasan, pemeriksaan, dan investigasi kecelakaan menurut hukum (7) Apabila pihak yang bersangkutan memiliki kemampuan untuk melaksanakan denda administratif atau penghargaan administratif tetapi tidak dapat melaksanakan atau menghindari eksekusi, yang secara serius mempengaruhi kredibilitas departemen pengawasan dan administrasi pasar, maka harus dimasukkan dalam daftar pelanggaran serius dan pelanggaran kepercayaan (8) Apabila undang-undang, peraturan administratif, dan dokumen kebijakan Komite Sentral BPK dan Dewan Negara menetapkan pencantuman orang yang relevan yang bertanggung jawab atas entitas pasar dalam daftar pelanggaran serius dan pelanggaran kepercayaan, ketentuan tersebut akan berlaku	

2. Pelanggaran Kepercayaan Secara Umum

Perilaku melanggar kepercayaan secara umum terutama mengacu pada perilaku melanggar kepercayaan yang ilegal dengan sifat kecil, keadaan kecil, dan tingkat kerugian sosial yang kecil. Perilaku umum yang melanggar kepercayaan ditunjukkan pada **Tabel 7.2**.

Tabel 7.2 Perilaku ketidakjujuran umum yang umum terjadi

Perilaku Melanggar Janji	Bidang Industri yang Terjadi
Perilaku kebingungan pasar, publisitas palsu, penipuan komersial, fitnah komersial, penyuapan komersial, dan tindakan ilegal lainnya	Bidang sirkulasi perdagangan
Penipuan keuangan, penghindaran jahat, dan pembatalan utang bank, perdagangan orang dalam, pembuatan dan penjualan polis asuransi palsu, penipuan asuransi, pengungkapan informasi palsu, penggalangan dana ilegal, penghindaran ke luar negeri, dan perilaku ketidakjujuran keuangan lainnya	Bidang keuangan
Tindakan ilegal dalam perpajakan. Hal ini mencakup penghindaran, penggelapan, dan penipuan lainnya	Bidang pajak
Pemalsuan dan penyebaran informasi kenaikan harga, penipuan harga, monopoli harga, dan perilaku lainnya	Bidang harga
Semua jenis pelanggaran transportasi	Bidang transportasi
Membuat dan menjual barang palsu, kegiatan penjualan piramida, iklan palsu, barang jelek, kegagalan layanan, dan penipuan lainnya; kolusi internal dan eksternal, memalsukan lalu lintas dan reputasi bisnis	E-Commerce
Penipuan	Bidang statistik
Semua jenis iklan palsu	Bidang pameran dan periklanan

Perilaku Melanggar Janji	Bidang Industri yang Terjadi
Tindakan ilegal penunggakan upah	Bidang tenaga kerja dan ketenagakerjaan
Semua jenis penipuan donasi dan perilaku yang melanggar kepercayaan lainnya, pelanggaran, penipuan, penipuan asuransi, dan perilaku lainnya	Bidang jaminan sosial

7.2 Penilaian dan Pengambilan Keputusan Risiko Kredit E-commerce

7.2.1 Gambaran Umum Evaluasi Kredit

Dalam evaluasi risiko kredit yang signifikan, tujuan utama dalam menilai pihak lain adalah untuk berinteraksi dengan entitas yang memiliki peringkat kredit lebih tinggi. Sementara itu, penilaian terhadap diri sendiri bertujuan untuk mengidentifikasi potensi risiko kredit, mengurangi atau menghilangkan kemungkinan tindakan yang tidak jujur, meningkatkan standar operasional, serta berupaya meningkatkan peringkat kredit secara keseluruhan.

Risiko kredit dan tingkat kredit merupakan dua aspek yang saling berkaitan dalam sistem evaluasi kepercayaan, yang masing-masing merepresentasikan sudut pandang berbeda mengenai kredibilitas. Sebagai contoh, jika ditinjau dari perspektif kredit, maka peringkat kredit seorang pelaku e-commerce dapat digunakan sebagai indikator keandalannya. Sebaliknya, dari sudut pandang risiko, peringkat kredit yang tinggi mencerminkan bahwa pelaku e-commerce memiliki risiko kredit yang lebih rendah. Pada dasarnya, tujuan utama dari penilaian risiko kredit dapat dicapai melalui proses evaluasi kredit. Mengacu pada standar nasional Sistem Indeks Evaluasi Kredit Pribadi dan Spesifikasi Presentasi Subjek Transaksi Berdasarkan Aktivitas E-commerce (GB/T 28041-2011), evaluasi kredit—atau yang sering disebut sebagai Penilaian Kredit—merupakan proses penilaian terhadap kapasitas serta kredibilitas suatu entitas secara objektif dan adil, yang kemudian dinyatakan dalam bentuk peringkat atau simbol tertentu. Selanjutnya, pembahasan akan mencakup prinsip-prinsip evaluasi kredit, pihak-pihak yang terlibat dalam proses penilaian, elemen yang menjadi dasar penilaian, serta indikator yang digunakan dalam evaluasi kredit.

1. Prinsip-Prinsip Evaluasi

Pertama, Prinsip evaluasi kredit perusahaan didasarkan pada beberapa aspek utama yang memastikan keakuratan dan keandalan penilaian. Prinsip komprehensif menekankan bahwa indeks evaluasi harus mencakup informasi utama yang dapat secara jelas mencerminkan kredibilitas suatu perusahaan. Prinsip sistemik menuntut agar setiap elemen dalam indeks evaluasi tidak berdiri sendiri atau tumpang tindih, melainkan saling melengkapi dalam sebuah

sistem yang utuh guna memberikan gambaran menyeluruh tentang status kredit perusahaan dalam ekosistem e-commerce. Sementara itu, prinsip pengoperasian memastikan bahwa indeks evaluasi kredit bersifat praktis, di mana setiap elemen yang dinilai harus memiliki karakteristik yang memungkinkan pengumpulan data yang akurat, dapat diukur, serta mudah diterapkan dalam proses evaluasi.

Selanjutnya, Evaluasi kredit individu dalam kegiatan e-commerce harus berlandaskan pada beberapa prinsip utama untuk memastikan transparansi dan akurasi dalam penilaian. Prinsip keadilan menekankan bahwa setiap individu memiliki kedudukan hukum yang setara, sehingga penyelenggara evaluasi harus memperlakukan semua subjek secara adil tanpa diskriminasi. Prinsip objektivitas mengharuskan proses penilaian dilakukan secara netral dan tidak memihak, sesuai dengan metode evaluasi yang telah ditetapkan. Prinsip keterbukaan memastikan bahwa sistem, metode, hasil, dan cara penyajian evaluasi kredit dapat diakses secara transparan, sehingga memudahkan pemangku kepentingan dalam memahami proses yang diterapkan. Sementara itu, prinsip ketepatan waktu menggarisbawahi pentingnya pemantauan kredit individu secara berkala, di mana setiap perubahan dalam transaksi e-commerce harus segera diperbarui agar hasil evaluasi tetap relevan dan akurat.

2. Evaluasi Para Peserta

Peserta evaluasi memiliki subjek evaluasi dan objek evaluasi. Pertama, subjek evaluasi. Operator e-commerce harus membangun dan meningkatkan sistem evaluasi kredit, mempublikasikan aturan evaluasi kredit, dan menyediakan cara bagi konsumen untuk mengevaluasi barang yang dijual atau layanan yang disediakan oleh platform e-commerce. Pekerjaan evaluasi kredit secara spesifik umumnya dilakukan oleh lembaga evaluasi kredit pihak ketiga yang dipercayakan. Subjek evaluasi meliputi konsumen, operator platform, subjek layanan, badan pengatur pemerintah, dan lembaga evaluasi kredit pihak ketiga.

Dalam ekosistem e-commerce, evaluasi dari konsumen memainkan peran penting dalam menentukan kredibilitas operator dan platform e-commerce. Evaluasi ini mencakup penilaian terhadap reputasi operator serta kualitas layanan yang mereka tawarkan. Dalam praktiknya, terdapat dua fenomena yang berlawanan terkait evaluasi konsumen, yaitu pujian palsu dan ulasan negatif yang tidak jujur. Pujian palsu terjadi ketika pihak penjual dan pembeli berkolaborasi untuk meningkatkan peringkat kredit mereka dengan memberikan ulasan positif tanpa adanya transaksi yang nyata. Praktik ini dapat mengganggu keseimbangan pasar, menciptakan persepsi yang keliru tentang kredibilitas suatu bisnis, dan meningkatkan risiko dalam operasional e-commerce. Sebaliknya, ulasan negatif yang tidak jujur merupakan bentuk persaingan tidak sehat di mana suatu pihak dengan sengaja memberikan ulasan buruk terhadap

produk atau layanan pesaing dengan tujuan merugikan mereka. Tindakan ini tidak hanya merugikan operator yang menjalankan bisnisnya secara jujur, tetapi juga berdampak pada validitas data evaluasi yang dimiliki oleh platform e-commerce. Lebih jauh, jika dibiarkan, praktik ini dapat menyesatkan konsumen serta merusak iklim bisnis yang sehat dalam perdagangan elektronik.

Dalam ekosistem e-commerce, evaluasi kredit dilakukan oleh berbagai pihak dengan cakupan yang berbeda-beda. Operator dalam platform bertanggung jawab menilai kredibilitas mereka sendiri, operator platform e-commerce, serta pihak lain seperti konsumen dan operator lain di dalam ekosistem yang sama.

Subjek layanan, yang mencakup berbagai penyedia jasa, juga menjadi objek evaluasi. Dalam hal ini, evaluasi meliputi penilaian terhadap operator platform e-commerce, penyedia layanan logistik dan distribusi, lembaga penyedia layanan pembayaran, serta berbagai penyedia jasa lainnya yang terlibat dalam transaksi e-commerce.

Selain itu, regulator pemerintah berperan dalam mengawasi dan mengevaluasi kredibilitas para pelaku transaksi e-commerce. Penilaian ini mencakup operator platform e-commerce, operator dalam platform, serta entitas lain seperti konsumen dan pelaku bisnis yang beroperasi di dalam maupun di luar platform tertentu. Evaluasi dari regulator bertujuan untuk memastikan kepatuhan terhadap regulasi yang berlaku serta menjaga kepercayaan dalam ekosistem perdagangan elektronik.

Lembaga evaluasi kredit pihak ketiga berperan dalam menilai kredibilitas setiap pelaku dalam transaksi e-commerce. Penilaian ini mencakup evaluasi terhadap status kredit lembaga itu sendiri serta pihak lain yang terlibat dalam ekosistem perdagangan elektronik. Operator e-commerce dapat melakukan penilaian kredit secara mandiri atau mempercayakan proses tersebut kepada lembaga pihak ketiga. Di sisi lain, regulator pemerintah memiliki kewajiban untuk menyediakan informasi terkait evaluasi kredit kepada seluruh peserta dalam transaksi e-commerce. Operator e-commerce dapat memperoleh data kredit dari lembaga pihak ketiga dengan biaya tertentu, sementara informasi kredit dari badan pengawas pemerintah dapat diakses secara gratis, baik untuk kebutuhan mereka sendiri maupun untuk mengetahui status kredit pihak lain yang relevan.

Kedua, objek evaluasi. Objek evaluasi dalam sistem kredit mencakup dua aspek utama, yaitu penilaian terhadap pihak lain dan evaluasi diri. Evaluasi terhadap pihak lain mencakup operator platform e-commerce, pelaku bisnis dalam platform, konsumen, serta peserta transaksi e-commerce lainnya. Dalam melakukan penilaian ini, informasi kredit dapat diperoleh melalui pembelian data dari lembaga evaluasi kredit pihak ketiga atau mengakses informasi yang

disediakan oleh badan pengawas pemerintah. Sementara itu, evaluasi diri merupakan proses penilaian terhadap kredibilitas sendiri, yang dapat dilakukan secara mandiri atau dengan bantuan lembaga evaluasi pihak ketiga untuk mendapatkan hasil yang lebih objektif dan komprehensif.

3. Elemen Evaluasi

Elemen evaluasi meliputi elemen evaluasi kredit perusahaan dan elemen evaluasi kredit individu.

Pertama, elemen evaluasi kredit perusahaan. Elemen evaluasi kredit perusahaan mencakup berbagai aspek penting yang mencerminkan legalitas dan kredibilitasnya. Informasi dasar mencakup data fundamental yang menegaskan keberadaan hukum suatu perusahaan, khususnya yang bergerak dalam aktivitas e-commerce. Selain itu, informasi kualifikasi menjadi faktor penting karena menggambarkan karakteristik khusus dari entitas perusahaan tersebut. Aspek lain yang turut diperhitungkan adalah informasi transaksi, yang mencerminkan besaran serta pencapaian dalam aktivitas perdagangan. Tak kalah penting, status kredit perusahaan serta hasil evaluasi kredit yang dilakukan oleh pihak ketiga juga menjadi indikator utama dalam menentukan tingkat kepercayaan terhadap perusahaan tersebut.

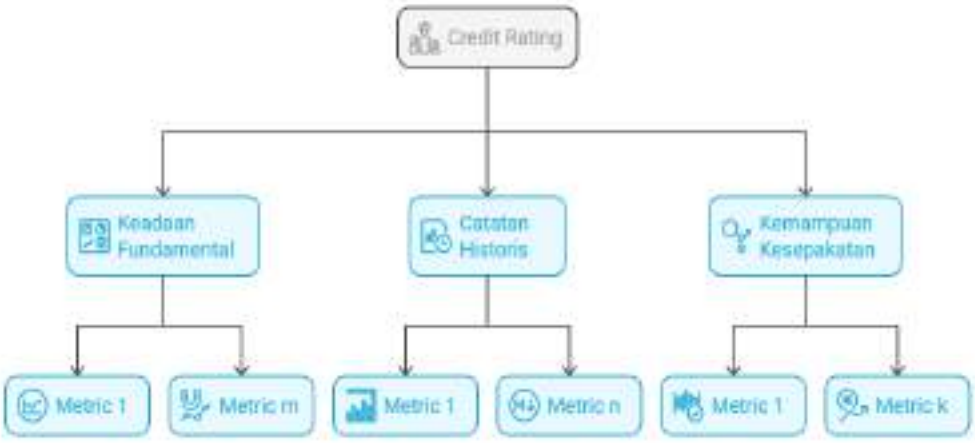
Kedua, elemen-elemen evaluasi kredit personal. Elemen-elemen evaluasi kredit pribadi didasarkan pada beberapa elemen utama, termasuk informasi dasar, transaksi, evaluasi, dan riwayat permintaan. Informasi dasar berfungsi untuk mengidentifikasi individu serta alamat situs web yang terkait, menjadikannya sebagai elemen fundamental dalam penilaian kredit pribadi. Proses evaluasi terhadap informasi dasar mencakup aspek keakuratan, keaslian, dan ketepatan waktu. Selain itu, informasi transaksi menjadi komponen penting, mencakup riwayat transaksi individu, pembayaran, kepatuhan terhadap kontrak, serta catatan terkait lainnya yang berkontribusi dalam menilai kredibilitas seseorang dalam e-commerce. Sementara itu, informasi evaluasi mencakup penilaian dari berbagai pihak dalam transaksi e-commerce, seperti ulasan dari mitra dagang, lembaga evaluasi kredit pihak ketiga, serta catatan pengaduan yang berfungsi sebagai referensi tambahan dalam menentukan tingkat kepercayaan individu. Terakhir, riwayat permintaan kredit merujuk pada rekam jejak kredit yang disimpan oleh instansi pemerintah, lembaga peradilan, atau institusi publik lainnya. Data ini meliputi informasi pembayaran pajak, pencapaian penghargaan, catatan negatif, serta aspek lainnya yang menjadi faktor utama dalam penilaian kredit pribadi dalam ekosistem e-commerce.

4. Indikator Evaluasi

Pertama, model dasar pemeringkatan kredit e-commerce. Model dasar pemeringkatan kredit e-commerce ditunjukkan pada **Gambar. 7.1**.

Indikator pemeringkatan kredit e-commerce dibagi menjadi dua jenis: indikator kualitatif dan indikator kuantitatif, indikator kualitatif dapat dihitung dengan metode evaluasi komprehensif fuzzy, buku ini tidak membahas secara rinci. Metode perhitungan indikator kuantitatif diperkenalkan di bawah ini. Rumus perhitungan indeks kuantitatif dalam peringkat kredit e-commerce adalah sebagai berikut:

$$F = \sum_{i=} w_i \sum_{j=} w_{ij} f_{ij}$$



Gambar 7. 1 Model dasar peringkat kredit E-commerce

Dalam rumus ini, *F* menunjukkan peringkat kredit, *wi* mewakili bobot *i* indeks evaluasi tingkat pertama, w_{ij} mewakili bobot *ij* indeks evaluasi tingkat kedua, *f(ij)* mewakili nilai *ij* indeks evaluasi tingkat kedua, n mewakili jumlah indikator evaluasi tingkat pertama, dan m mewakili jumlah indikator evaluasi tingkat kedua dari indeks evaluasi tingkat pertama.

Indeks evaluasi kredit perusahaan: Menurut Kode untuk Indikator Evaluasi Kredit dan Tingkat Subjek Transaksi Berdasarkan Aktivitas E-commerce (GB/T 26842- 2011), indikator evaluasi kredit perusahaan mencakup informasi dasar, informasi kualifikasi, informasi transaksi, informasi keuangan, informasi yang diminta, dan informasi evaluasi.

Indeks evaluasi kredit pribadi: Menurut Sistem Indeks Evaluasi Kredit Pribadi dan Standar Indeks Subjek Transaksi berdasarkan Aktivitas E-commerce (GB/T 28041- 2011), indeks evaluasi kredit pribadi dapat dibagi menjadi indeks peringkat kredit pribadi pembeli dan indeks

evaluasi kredit pribadi penjual. Indikator evaluasi kredit pribadi pembeli meliputi informasi dasar, informasi transaksi, informasi evaluasi, dan informasi permintaan.

Indeks evaluasi kredit pribadi penjual mencakup empat kategori: informasi dasar, transaksi, informasi evaluasi, dan informasi khusus.

Sistem indeks evaluasi kredit barang konsumsi: Menurut Sistem Indeks Evaluasi Kredit Ritel Jaringan Kredit E-commerce (GB/T 34056-2017), indikator evaluasi kredit online untuk jaringan barang konsumsi dan Indikator tingkat pertama dari evaluasi kredit ritel online untuk barang konsumsi. Perlu dicatat bahwa situs web ritel yang dioperasikan sendiri, dan toko online merujuk pada toko online pada platform ritel online pihak ketiga.

Ada tiga masalah utama dalam evaluasi kredit e-commerce: Pertama, sulit untuk memverifikasi keaslian evaluasi konsumen (pembeli). Sistem evaluasi kredit dari beberapa platform perdagangan online tidak dapat membedakan antara transaksi nyata dan transaksi palsu, meninggalkan celah untuk spekulasi kredit. Kedua, faktor referensi dalam evaluasi tidak lengkap. Dalam evaluasi kredit, penanganan keluhan konsumen dan hukuman administratif dari departemen terkait tidak termasuk dalam indikator evaluasi. Ketiga, otoritas penilaian tidak ditetapkan secara wajar. Sistem evaluasi kredit dari beberapa platform e-commerce membatasi konsumen untuk hanya memiliki satu kesempatan evaluasi setelah membeli barang, sehingga sulit untuk melindungi hak dan kepentingan konsumen ketika beberapa barang memiliki masalah dalam masa simpan.

Tabel 7.3 Pembeli

Fitur Evaluatif	**Indikator Evaluasi**	**Penjelasan**
Informasi dasar	Pernyataan informasi	Keakuratan dan keaslian semua jenis informasi dan materi yang diberikan kepada pihak ketiga
	Waktu pendirian perusahaan	Mencerminkan lamanya waktu perusahaan memperoleh status hukum dalam administrasi pengawasan pasar
	Waktu untuk lulus pemeriksaan dan persetujuan rekaman	Mencerminkan lamanya waktu yang dicatat oleh perusahaan di situs web

Fitur Evaluatif	Indikator Evaluasi	Penjelasan
		badan pengelolaan alam negara
	Laporan tahunan perusahaan	Laporan tahunan publik perusahaan
Informasi kualifikasi	Informasi kualifikasi lisensi administratif	Perusahaan telah memperoleh sertifikasi kualifikasi dari instansi pemerintah (sertifikat kualifikasi yang tidak valid dianggap tidak memenuhi syarat)
	Informasi kualifikasi lainnya	Perusahaan telah memperoleh sertifikasi kualifikasi dari lembaga yang berbeda (sertifikat kualifikasi yang tidak valid dianggap tidak memenuhi syarat)
Informasi perdagangan	Vitalitas	Termasuk waktu login pengguna, tingkat pembaruan informasi
	Akumulasi jumlah transaksi	Jumlah akumulasi dalam transaksi e-commerce ketika perusahaan berpartisipasi dalam evaluasi
	Frekuensi perdagangan	Transaksi e-commerce bulanan
	Tingkat jangkauan transaksi	Mencerminkan keberhasilan transaksi perusahaan dalam transaksi e-commerce

Fitur Evaluatif	Indikator Evaluasi	Penjelasan
	Tingkat realisasi transaksi	Mencerminkan keberhasilan penyelesaian transaksi dalam transaksi e-commerce
Informasi keuangan	Rasio aset-liabilitas	Mencerminkan proporsi total aset yang dibiayai melalui pinjaman
	Rasio lancar	Mencerminkan kemampuan likuiditas aset perusahaan
	Imbal hasil atas ekuitas	Mencerminkan tingkat pendapatan yang mendorong hak dan kepentingan
	Tingkat akumulasi modal	Mencerminkan kemampuan akumulasi modal perusahaan pada tahun berjalan
	Meningkatkan tingkat pendapatan bisnis	Mencerminkan situasi pertumbuhan pendapatan operasional perusahaan
Pesan yang cepat	Informasi yang buruk	Perusahaan melanggar hukum dan peraturan di lembaga sosial dan publik dan aspek lainnya
	Informasi kehormatan	Honor (kontrak dan judul kredit, honor merek dagang, honor perwakilan hukum, lanjutan pembayaran pajak, unit peradaban, kesejahteraan sosial, dll.)
Informasi evaluasi	Informasi evaluasi transaksi	Mencerminkan kinerja kontrak perusahaan dalam aktivitas e-commerce
	Informasi pengaduan	Merefleksikan keluhan perusahaan dalam e-

Fitur Evaluatif	Indikator Evaluasi	Penjelasan
		commerce termasuk kualitas dan layanan, informasi pelanggan dan manajemen data transaksi
	Informasi evaluasi (tingkat) kredit pihak ketiga	Peringkat bank atau peringkat kredit (dibagi dengan peringkat kredit sistem empat tingkat sepuluh atau peringkat yang sesuai)

7.2.2 Proses Evaluasi Risiko Kredit

1. Tahap persiapan evaluasi

Data yang digunakan dalam indikator evaluasi kredit sebagian besar dikutip dari data dalam file kredit perusahaan. Persiapan berikut ini harus dilakukan untuk evaluasi kredit. Pertama-tama, untuk memperjelas item data yang perlu dikumpulkan selama evaluasi kredit. Kedua, bobot indeks ditentukan sesuai dengan industri dan wilayah, dan sistem indeks evaluasi ditetapkan. Kemudian, indeks evaluasi, proses evaluasi, dan metode representasi tingkat hasil evaluasi dipublikasikan.

2. Tahap evaluasi awal

Pertama, pengumpulan informasi. Informasi kredit perusahaan dapat dikumpulkan dengan komputer atau secara manual. Subjek pengumpulan informasi kredit terutama mencakup pemerintah, departemen, lembaga layanan kredit, dan organisasi industri. Departemen pemerintah memiliki banyak informasi, beberapa di antaranya dibagikan. Lembaga layanan kredit adalah pelaku utama pengumpulan informasi. Mereka mengumpulkan informasi transaksi yang relevan dari subjek transaksi e-commerce, dan menjual atau mengungkapkan informasi kredit transaksi yang relevan dengan membuat tanda kredit khusus e-commerce mereka sendiri. Organisasi industri memiliki sejumlah besar informasi produksi, perdagangan, dan pasar industri.

Kedua, hasil evaluasi awal. Subjek evaluasi menganalisis dan menghitung data yang dikumpulkan dari perusahaan e-commerce, dan memperoleh hasil evaluasi awal peringkat kredit perusahaan e-commerce menurut sistem indeks evaluasi dan klasifikasi peringkat kredit.

Ketiga, pemberitahuan publik. Hasil evaluasi awal akan dipublikasikan di situs web untuk jangka waktu tidak kurang dari 15 hari, dan cara menerima keberatan akan dipublikasikan.

3. Tahap evaluasi akhir

Salah satunya adalah evaluasi akhir. Jika perusahaan e-commerce tidak keberatan dengan hasil evaluasi selama periode publisitas evaluasi awal, hasil evaluasi awal adalah peringkat kredit akhir perusahaan e-commerce. Setelah periode publisitas berakhir, peringkat kredit akhir perusahaan e-commerce akan dirilis secara resmi, dan tanggal evaluasi terbaru dari peringkat kredit akan ditunjukkan.

Tabel 7.4 Indeks evaluasi kredit pribadi penjual

Kelas	Indikator Evaluasi	Penjelasan
Informasi penting	Nama asli pengguna	Untuk mengevaluasi penggunaan nama asli, nama bersih (nama pena), atau nama lain dari identitas pribadi penjual selama pendaftaran di platform layanan e-commerce atau lembaga terkait
	Kode identifikasi entitas utama kredit	Untuk mengevaluasi akurasi, keaslian, dan ketepatan waktu dari semua jenis informasi dan materi yang diberikan oleh penjual kepada platform layanan e-commerce atau lembaga terkait
	Informasi kontak	
	Pernyataan informasi	
	Waktu pendaftaran	Lamanya waktu penjual memperoleh status hukum di negara platform layanan e-commerce atau lembaga terkait harus dievaluasi
	Pengarsipan informasi	Untuk mengevaluasi situasi pencatatan penjual perorangan (industri perorangan dan rumah

Kelas	Indikator Evaluasi	Penjelasan
		tangga komersial) di departemen pemerintah terkait
	Informasi lainnya	Tinjau informasi tambahan sesuai kebutuhan
Informasi perdagangan	Jumlah transaksi kumulatif tahunan	Untuk mengevaluasi akumulasi jumlah transaksi penjual dalam transaksi e-commerce tertentu pada tahun tertentu
	Rata-rata waktu transaksi bulanan	Untuk mengevaluasi jumlah rata-rata transaksi e-commerce bulanan penjual pada tahun sebelumnya
	Jumlah transaksi	Nilai jumlah transaksi yang dicapai oleh penjual dalam transaksi e-commerce
	Informasi online	Waktu online penjual di aktivitas e-commerce dievaluasi dengan pemeriksaan langsung. Seperti pada online penuh waktu harian, online reguler harian, online tidak reguler
	Iklan	Untuk mengevaluasi apakah barang atau jasa yang disediakan oleh penjual dipublikasikan secara berlebihan
	Pembaruan informasi	Untuk mengevaluasi ketepatan waktu publisitas barang atau jasa yang

Kelas	Indikator Evaluasi	Penjelasan
		disediakan oleh penjual secara pribadi
	Jaminan barang atau jasa	Evaluasi ketepatan waktu atau ketepatan waktu barang atau jasa yang disediakan oleh penjual
	Informasi faktur	Untuk mengevaluasi apakah akan menerbitkan faktur Anda sendiri
	Informasi lainnya	Evaluasi informasi yang relevan dari partisipasi pribadi penjual dalam operasi e-commerce
Informasi evaluasi	Evaluasi pihak transaksi	Untuk mengevaluasi kinerja kontrak pribadi penjual dalam aktivitas e-commerce
	Keluhan pihak yang bertransaksi	Menurut pembeli untuk mengevaluasi keluhan wanprestasi pribadi penjual (tidak termasuk kualitas keluhan)
	Keluhan kualitas	Untuk mengevaluasi keluhan tentang kualitas barang dan jasa yang disediakan oleh penjual
	Evaluasi penyedia layanan platform	Pihak ketiga (penyedia layanan platform) akan mengevaluasi penjual individu
	Evaluasi kredit pihak ketiga sosial	Evaluasi terkait kredit yang diberikan oleh bank, lembaga kredit, industri, dan

Kelas	Indikator Evaluasi	Penjelasan
		pemerintah terkait departemen administrasi
Informasi khusus	Informasi pajak	Untuk mengevaluasi situasi pembayaran pajak perorangan penjual menurut hukum
	Informasi kualifikasi	Untuk mengevaluasi pencapaian penjual terhadap otoritas kompeten yang relevan dalam hal izin usaha dan kualifikasi
	Informasi kehormatan	Evaluasi catatan kredit penjual di departemen pemerintah, lembaga peradilan, atau lembaga sosial masyarakat lainnya
	Catatan perilaku buruk	
	Informasi lainnya	Evaluasi informasi khusus lainnya yang perlu ditambahkan sesuai dengan situasi aktual

Tabel 7.5 Indeks utama evaluasi kredit ritel online untuk barang konsumsi

Indikator Level 1	Persyaratan dan petunjuk umum	Index nilai penuh
Legitimasi bisnis	Indeks ini adalah indeks ambang batas untuk mengevaluasi kredit ritel online, dan mengevaluasi kredit ritel online kredit ritel harus dipenuhi: (1) Operator memiliki identitas ritel online yang sah; (2) Situs web/toko online yang dievaluasi tidak memiliki pelanggaran serius terhadap hukum dan peraturan Evaluasi tanpa	(veto)

	pengecualian untuk indeks ini akan langsung dinilai baik di bawah ini (tidak termasuk baik)	
Status operasi	Situs web/toko online yang beroperasi secara terus menerus, dengan volume perdagangan tertentu	10
Pengungkapan informasi	Deskripsi yang akurat dan jelas mengenai produk yang dijual, harga, dan biaya	20
Kualitas produk	Produk yang diperoleh pelanggan (termasuk layanan pemasangan dan pemeliharaan yang ditetapkan oleh sistem sertifikasi produk wajib atau dijanjikan oleh penjual) konsisten dengan deskripsi dan harapan yang dihasilkan sebelum pelanggan menjelajahi situs web/toko online	20
Layanan yang memadai dan sistematis	Persyaratannyq adalah sebagai berikut: (1) Metode pembayaran yang nyaman dan aman (2) Pengiriman/penyerahan mencapai tingkat yang dijanjikan dan harapan pelanggan (3) Layanan pengembalian dan penukaran tidak boleh lebih rendah dari peraturan perundang-undangan yang berlaku dan komitmen penjual (4) Pengoperasian situs web/toko online yang jujur harus diakui oleh pelanggan yang berbelanja	20
Evaluasi komprehensif dan pengaduan eksternal	Indeks ini dijelaskan sebagai berikut: (1) Evaluasi komprehensif atas kepercayaan pelanggan terhadap situs web atau toko online adalah data positif yang mencerminkan kredit komprehensif (2) Keluhan dari luar situs web atau oleh platform adalah data negatif yang mencerminkan kredit yang komprehensif	30

	(3) Kedua data tersebut dapat diganti satu sama lain atau dengan indikator level 1 lainnya secara keseluruhan	

Tabel 7.6 Indikator sekunder evaluasi kredit ritel online untuk barang konsumsi

Indikator Level 1	**Indikator sekunder**	**Deskripsi indikator sekunder**	**Index nilai penuh**	**Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)**
Bisnis legitimas	Entitas operator kualifikasi/identitas	Verifikasi sertifikat badan hukum dan dokumen identitas	(Veto)	Verifikasi melalui data yang disediakan oleh pemerintah dan pengadilan; (1) Situs web: verifikasi keaslian dan keabsahan izin usaha, sertifikat badan hukum, dan catatan ICP atau izin usaha ICP situs web; jangan memverifikasi sertifikat badan hukum dan memverifikasi keaslian dan keabsahan identitas sertifikat; (2) Toko online: verifikasi keaslian dan keabsahan sertifikat identitas pendaftar toko online dan izin usaha dari agen pendaftaran;
	Pengarsipan Layanan Informasi Internet (ICP) dan perizinan	Verifikasi pengajuan ICP atau izin usaha ICP		
	Perizinan administratif	Verifikasi izin usaha, ritel industri khusus membutuhkan izin administratif yang relevan		
	Catatan kriminal atas pelanggaran serius terhadap hukum dan peraturan	Situs web/toko dalam waktu tiga tahun apakah ada pornografi, perjudian, narkoba, penjualan piramida, penipuan, pelanggaran impor dan ekspor, dan jenis pelanggaran serius		

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
		lainnya terhadap hukum dan peraturan catatan hukuman		(3) Catatan kriminal atas pelanggaran hukum dan peraturan Evaluasi kredit tidak akan diberikan dalam waktu 3 tahun untuk kasus-kasus kualifikasi/informasi identitas yang tidak konsisten, tidak memiliki izin administratif, dan catatan kriminal dan ilegal yang serius
Status operasi	Mulai jam kerja	Periksa situs web/toko online yang beroperasi tahun ritel online, tidak termasuk bisnis e-commerce ritel non-online dan bisnis offline	4	Empat poin selama tiga tahun, 2 poin per tahun, 1 poin selama setengah tahun, kurang dari setengah tahun, 0 poin
	Aktivitas perdagangan terkini	Melihat volume kumulatif atau volume dalam 3 bulan terakhir	6	(1) Situs web: jumlah transaksi mencapai 10.000 atau 5.000 dan volume transaksi mencapai 6 poin; transaksi mencapai 5.000 atau 2.500.000.100.000;

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
				lainnya dihitung 0 poin; (2) Toko online: jumlah transaksi mencapai 1000 atau 500:500 atau 250.200 atau 100.100 atau 50 dan 5000; 0 poin; Jika data volume tidak tersedia, ganti situs (kunjungan IP harian/5)
Pengungkapan informasi	Deskripsi produk	Evaluasi deskripsi lengkap dari atribut utama produk	10	Menurut umpan balik pembeli dan evaluasi data survei sampel, deskripsi sangat memadai 10 poin, relatif memadai 7 poin, tidak memadai 4 poin, sangat tidak memadai 0 poin
	Tanda harga produk	Untuk mengevaluasi tingkat pelabelan harga produk yang jelas, benar, dan akurat, serta tidak menyesatkan	4	Skor penuh adalah 4 poin. Menurut umpan balik pembeli dan evaluasi data survei sampel, 1-2 poin akan dikurangi sesuai dengan tingkat keparahannya, dan ada ketidakkonsistenan yang menyesatkan antara harga dan pembayaran aktual (diperbolehkan untuk menegosiasikan pengurangan

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
				harga pembayaran dan meningkatkan diskon). 1-4 poin akan dikurangi sesuai dengan tingkat keparahannya, dan total 4 poin akan dikurangi
	Petunjuk terkait pengiriman produk	Jelaskan lokasi pengiriman produk dan waktu kedatangan yang diharapkan secara jelas di halaman web	2	Untuk semua kategori produk yang dijual di situs web / toko online, 10 halaman deskripsi produk diperiksa secara acak secara proporsional (kurang dari 10 tampilan semua, dievaluasi secara proporsional), dan tempat pengiriman dan waktu kedatangan diharapkan menunjukkan 2 poin, 1-3 tidak ditandai 1 poin, dan lebih dari 3 tidak ditandai 0 poin
	Tanda biaya pengiriman	Tandai biaya pengiriman dengan jelas di sebelah harga produk pada halaman deskripsi produk	2	Untuk semua kategori produk yang dijual di situs web/toko, 10 halaman deskripsi produk (kurang dari 10 lihat semua, evaluasi berdasarkan proporsi), semua menunjukkan standar biaya pengiriman 2 poin, 1-3 tanpa tanda 1 poin, lebih dari 3 tanpa tanda 0 poin; situs

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
				web/toko semua produk bebas biaya pengiriman 2 poin
	Tanda biaya purna jual	Layanan purna jual (seperti pemasangan, pemeliharaan, pengembalian dan penukaran, dll., akuisisi dan standar pengisian) ditandai jelas di sebelah harga produk pada halaman deskripsi produk	2	Untuk semua kategori produk yang dijual di situs web / toko online, 10 halaman deskripsi produk diperiksa secara acak secara proporsional (kurang dari 10 tampilan semua, dievaluasi secara proporsional), semua menunjukkan metode akuisisi layanan purna jual dan standar pengisian daya 2 poin, 1-3 poin 1 poin, lebih dari 3 poin 0 poin
Kualitas produk	dengan deskripsi gelar	Untuk mengevaluasi konsistensi produk yang dikirim (termasuk layanan purna jual yang ditentukan atau dijanjikan, seperti pemasangan dan pemeliharaan) dengan deskripsi teks dan gambar produk yang disediakan oleh situs web/toko online, dan	12	Menurut umpan balik pembeli dan evaluasi data sampel, kualitas produk cocok dengan tingkat deskripsi: sangat konsisten atau kelebihan cocok dengan 12 poin, semua karakteristik penting cocok dengan 9 poin, karakteristik terpenting cocok dengan 6 poin, setengah atau sebagian besar karakteristik penting tidak cocok dengan 0-3 poin. Poin juga dapat

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
		konsultasi, balasan, dan komitmen staf layanan situs web/toko online		dinilai dengan tingkat rata-rata
	Sesuai dengan harapan	Kualitas produk yang dikirimkan kepada Pembeli (termasuk purnajual yang ditentukan atau dijanjikan layanan, seperti pemasangan dan pemeliharaan) memenuhi tingkat yang diharapkan ketika pembeli melakukan pemesanan	8	Menurut umpan balik Pembeli dan evaluasi data sampel, 8 poin dihitung untuk kualitas keseluruhan dan ekspektasi pembeli di atas 80%, 6 poin untuk 60-80% (tidak termasuk 80%), 4 poin untuk 40-60% (tidak termasuk 60%) dan 0 poin untuk kurang dari 40%. Poin juga dapat dinilai berdasarkan tingkat rata-rata
Layanan Memadai dan sistematis	Legitimasi pembayaran online	Periksa keabsahan lisensi pembayaran pihak ketiga yang digunakan	1	Semua merchant pembayaran online opsional memiliki lisensi pembayaran pihak ketiga yang sah secara hukum, atau 0
	Tunai pada saat pengiriman	Periksa apakah sebagian besar item didukung dengan pembayaran tunai saat pengiriman	1	Untuk semua kategori produk yang dijual di situs web/toko online, 10 produk dipilih secara acak secara proporsional, dan lebih dari 8 produk (termasuk 8 produk) akan mendukung 1 poin, jika tidak, 0 poin

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
	Waktu kedatangan pengiriman	Ketika situs web / toko online memberikan ekspektasi waktu kedatangan, ia dapat mengevaluasi tingkat kepuasan sesuai dengan apakah situs web / toko online mencapai deskripsi atau tidak, tetapi apakah harapan pelanggan tercapai atau tidak	8	Inspeksi acak terhadap 10 verifikasi pesanan yang telah selesai, 8-10 kali untuk memenuhi persyaratan komitmen situs web/toko 8 poin, 6-7 kali untuk memenuhi persyaratan komitmen 6 poin, 4-5 kali untuk memenuhi persyaratan komitmen 4 poin, kurang dari 4 kali 0 poin; Ketika tidak ada ekspektasi waktu pengiriman yang jelas, apakah ekspektasi waktu kedatangan pembeli diganti
	Layanan pengembalian dan penukaran	Evaluasi (akses yang mudah dan efek layanan) memenuhi persyaratan komitmen/ekspektasi pelanggan; dengan komitmen layanan pengembalian dan penukaran yang jelas, evaluasi dapat dilakukan sesuai dengan persyaratan komitmen; Namun, dengan komitmen layanan purna jual	10	(1) Situs web/toko online tidak menyediakan layanan pengembalian dan penukaran sesuai dengan hukum dan peraturan nasional yang berlaku; (2) Menurut umpan balik pembeli, data sampel, pembeli mengajukan permohonan layanan purna jual dari kenyamanan dan efek layanan hingga

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
		yang jelas, evaluasi dapat didasarkan pada apakah harapan pelanggan		komitmen situs web / toko, lebih dari 90% (90%) untuk situs web / toko menjanjikan 10 poin, 80% (80%) menjanjikan 8 poin, 70-80% (70%) menjanjikan 6 poin, 60-70% (termasuk 60%) menjanjikan 4 poin, kurang dari 60% untuk menjanjikan 0-2 poin; (3) Data survei pengambilan sampel dapat digunakan untuk menghitung layanan purna jual untuk mencapai tingkat yang diharapkan pelanggan (atau kepuasan pelanggan layanan purna jual) sebagai gantinya
Evaluasi komprehensif dan di luar lokasi keluhan	Evaluasi komprehensif atas kepercayaan pelanggan	Setelah berbelanja, evaluasi atau nilai keseluruhan pelanggan terhadap	15	Berdasarkan umpan balik pelanggan dan data sampel, evaluasi kredibilitas situs web/toko online setelah pengalaman berbelanja; 15

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
		kredibilitas situs web/toko online		poin, 12 poin, 9 poin, 6 poin, dan 0-3 poin
	Situs web: Jumlah keluhan dari luar situs Toko online: jumlah pelanggan yang mengajukan keluhan ke platform	Ketika pelanggan mengalami perselisihan di dalam situs web atau bernegosiasi dengan toko online, mereka sering kali mengajukan keluhan kepada pihak ketiga di luar stasiun, pemerintah, atau platform; menghitung tingkat keluhan dari keluhan non-penjual Indeks ini tidak termasuk negosiasi atau permintaan bunga dari pelanggan dengan situs web perdagangan atau toko online	15	(1) Statistik jumlah keluhan efektif situs web/toko online di organisasi pihak ketiga atau departemen dan platform pemerintah dalam satu tahun terakhir. Dalam 1 tahun (jumlah keluhan/transaksi efektif), 15 poin tidak 50% di atas rata-rata industri, 50% tetapi kurang dari 70%, 9 poin di atas rata-rata; 0 poin di atas 2 kali lipat, 1,4 kali lipat tetapi tidak dua kali lipat dari ratarata, 6 poin di atas rata-rata tetapi tidak 1,4 kali lipat dari rata-rata; (2) Ketika tidak ada data rata-rata, tingkat pengaduan 15 poin lebih rendah dari (termasuk) 0,1%, 12

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
				poin di bawah (termasuk) 0,3%, 9 poin lebih rendah dari 0,5% (termasuk), 6 poin lebih rendah dari 0,7% (termasuk), 3 poin lebih rendah dari 1% (termasuk 1%), dan 0 poin lebih tinggi dari (tidak termasuk) 1%. Tingkat pengaduan statistik harus mencakup setidaknya 90% dari data platform penerimaan pengaduan pemerintah dan lembaga lokal yang relevan, dan juga dapat diperkirakan dengan menggunakan data sampel pelanggan
	Catatan ketidakjujuran dan hukuman	Periksa catatan yang relevan dalam waktu 1 tahun, termasuk hukuman administratif, toko online yang dihukum	Poin	(1) Dalam satu tahun terakhir, ketika situs web/toko online dihukum satu kali oleh departemen pemerintah, atau

Indikator Level 1	Indikator sekunder	Deskripsi indikator sekunder	Index nilai penuh	Aturan penilaian (dengan skor kontinu dan data serta metode lainnya)
		oleh platform atau dituntut, dll., Mengevaluasi tingkat ketidakjujuran sesuai dengan jumlah dan tingkat keparahan evaluasi, dan mengurangi skor pengaduan		kalah dalam gugatan satu kali, 1-8 poin akan dikurangi sesuai dengan tingkat keparahan kerugian dan kejahatan subjektif; (2) Dalam satu tahun terakhir, toko online akan dihukum satu kali oleh platform, dan 1 poin-4 poin akan dikurangi sesuai dengan tingkat keparahan kerusakan atau keburukan subyektif; (3) Hingga skor kumulatif maksimum dari indeks keluhan dikurangi (skor evaluasi komprehensif kepercayaan pelanggan tidak dikurangi). Anda dapat mengacu pada volume perdagangan saat menilai

Kedua, evaluasi ulang. Jika perusahaan e-commerce memiliki keberatan terhadap hasil evaluasi awal, dan dapat memberikan materi tambahan yang cukup dan efektif dalam batas waktu yang ditentukan, subjek evaluasi harus mengevaluasi materi tambahan yang diberikan oleh perusahaan e-commerce, yaitu evaluasi ulang. Evaluasi ulang hanya dibatasi satu kali, hasil evaluasi ulang akan dipublikasikan, dan hasil penilaian ulang adalah peringkat kredit akhir perusahaan e-commerce. Jika perusahaan e-commerce keberatan dengan hasil evaluasi, tetapi tidak dapat memberikan materi tambahan yang cukup dan efektif dalam batas waktu yang ditentukan, subjek evaluasi mungkin tidak menerima permintaan evaluasi ulang.

Yang ketiga adalah pelacakan. Menindaklanjuti perusahaan e-commerce yang dievaluasi secara teratur atau tidak teratur. Informasi kredit dikumpulkan berulang kali, dan informasi yang relevan dikirimkan ke sistem evaluasi dan penyelidikan kredit. Setelah analisis kualitatif dan kuantitatif, tingkat evaluasi kredit terbaru diberikan.

4. Nilai Evaluasi dan Perubahan

Pertama, peringkat kredit perusahaan e-commerce. Hasil evaluasi kredit perusahaan e-dagang dapat dibagi menjadi lima nilai, dari tinggi ke rendah dengan "lima bintang", empat", bintang tiga", bintang dua", dan "bintang satu", dan simbol kelas diwakili oleh nomor yang sesuai dari "★ ". Simbol kelas dapat disesuaikan dengan situasi yang sebenarnya, tetapi transformasi dan korespondensi dengan ini simbol standar harus ditunjukkan dengan jelas. Menurut Kode untuk Indeks Evaluasi Kredit dan Representasi Nilai Perusahaan Subjek Transaksi Berdasarkan Aktivitas E-commerce (GB/T 26842-2011), representasi peringkat kredit ditunjukkan pada **Tabel 7.7**.

Kedua, peringkat kredit pribadi. Hasil evaluasi kredit pribadi dapat dibagi menjadi lima tingkatan, yaitu "bintang lima", "bintang empat", "bintang tiga", bintang dua", "bintang dua", dan "bintang tiga". bintang" dan "satu bintang". Perbedaan level tercermin dari jumlah simbol "★ ". Menurut Sistem Indeks Evaluasi Kredit Personal dan Spesifikasi Indeks Subjek Transaksi Berdasarkan Aktivitas Perdagangan Elektronik (GB/T 28041-2011), representasi dan deskripsi peringkat kredit individu ditunjukkan pada **Tabel 7.8**.

Dalam lingkungan transaksi e-commerce yang sebenarnya, peringkat kredit objek transaksi tidak selalu lima bintang atau nilai yang lebih tinggi, dll. Peringkat kredit yang rendah tidak berarti tidak layak untuk diperdagangkan, selama masih dalam kisaran yang dapat dikontrol. Tentu saja, dalam kondisi yang sama, tidak ada peningkatan biaya yang harus diprioritaskan dengan transaksi objek transaksi dengan peringkat kredit yang tinggi.

Tabel 7.7 Representasi dan deskripsi peringkat kredit Perusahaan

Pesan	Kelas	Simbol Kelas	Penjelasan
1	Bintang lima	★★★★★	Status kredit yang sangat baik
2	Bintang empat	★★★★	Status kredit yang baik
3	Bintang tiga	★★★	Status kredit yang baik
4	Bintang dua	★★	Status kredit adalah umum
5	Bintang satu	★	Status kredit yang memenuhi syarat

Tabel 7.8 Presentasi dan deskripsi peringkat kredit individu

Pesan	Kelas	Simbol Kelas	Arti
1	Bintang lima	★★★★★	Peringkat kredit tertinggi
2	Bintang empat	★★★★	Peringkat kredit yang tinggi
3	Bintang tiga	★★★	Peringkat kredit yang tinggi
4	Bintang dua	★★	Peringkat kredit yang baik
5	Bintang satu	★	Individu tersebut telah memiliki file kredit atau peringkat kredit umum

Ketiga, nilai evaluasi harus berubah. Jika objek yang dievaluasi tidak memperbarui informasi kredit dalam waktu 6 bulan, maka peringkat evaluasi kredit akan dibatalkan. Ketika informasi tertentu atau peristiwa tertentu dapat menyebabkan perubahan peringkat kredit dari objek yang dievaluasi, hasil evaluasi peringkat kredit harus secara aktif diperiksa ulang atau dibatalkan.

7.2.3 Pengambilan Keputusan Pengendalian Risiko Kredit

Dalam sistem ekonomi pasar, kredit memainkan peran fundamental sebagai dasar dalam penerapan aturan hukum. Namun, karena sifatnya yang rentan, kredit menjadi sumber daya yang relatif langka, terutama dalam dunia perdagangan elektronik. Kepercayaan dalam e-commerce memiliki nilai yang tinggi, sehingga pengelolaan risiko kredit menjadi faktor kunci dalam memastikan standar dan keteraturan dalam industri ini. Dengan adanya kontrol yang efektif terhadap risiko kredit, e-commerce dapat berkembang secara sehat dan berkelanjutan. Pengendalian risiko kredit sendiri terbagi ke dalam beberapa kategori utama, yaitu pengendalian risiko kredit oleh perusahaan e-commerce, pengawasan oleh pemerintah, serta pengendalian yang dilakukan oleh lembaga pihak ketiga.

Pertama, pengendalian risiko kredit perusahaan e-commerce. Perusahaan e-commerce perlu membangun sistem kredit yang komprehensif dan terstruktur untuk mengawasi serta mengelola aktivitas para pelaku transaksi dalam ekosistem mereka. Terdapat empat pendekatan utama dalam pengendalian risiko kredit, yaitu mode perantara, mode penjamin, mode operasi situs web, dan mode otorisasi yang dipercayakan. Keempat metode ini bergantung pada kredibilitas peserta transaksi serta platform e-commerce itu sendiri. Platform mengumpulkan data kredit pengguna, menetapkan kebijakan, dan menentukan nilai kredit mereka, sehingga membentuk sistem penilaian sendiri. Namun, aturan dalam skema ini umumnya bersifat internal perusahaan dan tidak selalu memiliki stabilitas maupun otoritas hukum yang kuat.

Kedua, pengendalian risiko kredit oleh pemerintah. Pemerintah memiliki peran penting dalam memastikan transparansi dan keamanan ekosistem e-commerce dengan memperkuat pengawasan terhadap aktivitas bisnis perusahaan e-commerce serta mendorong mereka untuk meningkatkan sistem kredit dan pengawasan internal. Pemerintah juga bertanggung jawab dalam meningkatkan keandalan sistem kredit personal dengan menerapkan kebijakan yang mendukung lingkungan transaksi yang aman dan terpercaya. Beberapa langkah yang dapat dilakukan meliputi pengembangan lembaga layanan kredit, penerapan sanksi bagi pihak yang tidak jujur, serta pembangunan sistem sertifikasi kualifikasi bagi pelaku usaha e-commerce. Selain itu, pemerintah dapat memanfaatkan platform digital untuk autentikasi identitas dan menunjuk lembaga pihak ketiga yang bertugas menyimpan data terkait di internet. Dengan pendekatan ini, keamanan transaksi e-commerce dapat lebih terjamin, baik dari aspek teknis maupun hukum.

Ketiga, pengendalian risiko kredit pihak ketiga. Untuk memastikan transparansi dalam sistem kredit e-commerce, diperlukan lembaga layanan kredit pihak ketiga yang kredibel, profesional, dan memiliki legitimasi yang kuat. Lembaga ini dapat dikategorikan sebagai

lembaga layanan kredit personal dan lembaga layanan kredit perusahaan. Dengan adanya institusi evaluasi kredit independen yang berstatus badan hukum, layanan penilaian kredit dapat dilakukan secara lebih objektif dan adil, sehingga meningkatkan kepercayaan dalam transaksi e-commerce secara keseluruhan.

1. Pengambilan keputusan pengendalian risiko kredit

Dalam pengambilan keputusan terkait pengendalian risiko kredit, langkah pertama yang perlu dilakukan adalah memperkuat regulasi yang relevan. Pembangunan sistem hukum yang kokoh serta penyusunan dan penyempurnaan peraturan menjadi landasan utama dalam pembentukan serta penerapan sistem kredit sosial dan manajemen. Saat ini, lingkungan kredit di China masih memerlukan peningkatan lebih lanjut, yang dapat diwujudkan melalui perumusan undang-undang serta regulasi khusus yang lebih komprehensif.

Langkah selanjutnya adalah membangun mekanisme pengendalian risiko kredit yang efektif. Mekanisme ini mencakup sistem sanksi bagi perilaku yang melanggar kepercayaan, sistem insentif bagi pelaku usaha yang menjunjung tinggi integritas, serta mekanisme koordinasi yang tepat untuk memastikan keseimbangan dalam ekosistem kredit.

Selain itu, membangun budaya integritas juga menjadi aspek krusial dalam pengendalian risiko kredit. Budaya ini tidak dapat terbentuk secara alami, melainkan harus dikembangkan melalui upaya berkelanjutan. Pendidikan mengenai moralitas dan etika integritas serta penerapan sistem yang mendukung nilai-nilai kejujuran dapat menjadi instrumen utama dalam menciptakan lingkungan bisnis yang sehat dan terpercaya.

7.3 Implementasi Pengendalian Risiko Kredit E-commerce

Pengendalian risiko kredit e-commerce, pada dasarnya atau untuk mempromosikan pembangunan integritas sosial, membangun dan meningkatkan sistem jaminan kredit sosial. Menetapkan sistem insentif bersama untuk menjaga kepercayaan dan sistem hukuman bersama untuk menjaga pelanggaran kepercayaan, karena mekanisme hukuman untuk melanggar kepercayaan dapat menghilangkan risiko kredit perusahaan, dan mekanisme insentif untuk menjaga kepercayaan dapat mendorong perusahaan untuk mematuhi hukum dan beroperasi dengan itikad baik.

7.3.1 Memandu Ideologi dan Prinsip-prinsip Dasar

Pendekatan utama dalam pengendalian risiko kredit e-commerce adalah mempercepat pembangunan sistem kredit sosial, meningkatkan transparansi, serta mendorong pertukaran informasi kredit secara luas. Dengan menerapkan insentif bagi pihak yang memiliki rekam jejak kredit yang baik serta memberikan sanksi kepada pelanggar sesuai dengan regulasi yang

berlaku, diharapkan para pelaku usaha dapat beroperasi secara jujur dan sesuai hukum. Upaya ini bertujuan untuk menjaga stabilitas pasar dan menciptakan lingkungan bisnis yang berbasis integritas.

Terdapat beberapa prinsip dasar dalam pengelolaan risiko kredit e-commerce. Pertama, sistem penghargaan bagi pihak yang menjunjung tinggi integritas serta pemberian sanksi bagi mereka yang melanggar kepercayaan. Dengan menerapkan mekanisme ini, diharapkan pelaku bisnis yang bertindak jujur mendapatkan manfaat, sementara mereka yang melakukan pelanggaran akan menghadapi pembatasan. Hal ini bertujuan membangun sistem yang secara efektif mendorong kejujuran dan menekan pelanggaran kepercayaan. Kedua, adanya koordinasi antar lembaga serta keterlibatan masyarakat dalam sistem pengelolaan risiko kredit. Transparansi informasi kredit perlu diperkuat dengan membangun sistem insentif dan sanksi yang dapat diterapkan lintas sektor, wilayah, dan instansi terkait. Dengan demikian, akan tercipta ekosistem yang melibatkan sinergi antara pemerintah, organisasi industri, lembaga layanan kredit, serta kontrol sosial dari opini publik. Ketiga, perlindungan terhadap hak dan kepentingan individu sesuai dengan regulasi yang berlaku. Hal ini mencakup penyusunan definisi yang jelas mengenai tindakan yang mencerminkan kejujuran serta mekanisme pemberian insentif bagi pelaku bisnis yang menjaga kepercayaan. Selain itu, perlu ada sistem pemulihan kredit dan mekanisme pengajuan keberatan untuk melindungi hak-hak pihak yang terdampak. Keempat, fokus pada sektor-sektor utama yang memiliki dampak signifikan terhadap perekonomian dan masyarakat secara keseluruhan. Dalam hal ini, pemerintah serta lembaga terkait didorong untuk melakukan inovasi dalam sistem kredit guna menekan pelanggaran kepercayaan. Secara bertahap, mekanisme ini akan diterapkan ke seluruh sektor ekonomi dan sosial untuk menciptakan lingkungan bisnis yang lebih sehat dan terpercaya.

7.3.2 Mekanisme Pengendalian Risiko Kredit

Risiko kredit dapat dikendalikan dengan mekanisme membatasi dan menghukum perilaku yang melanggar kepercayaan, mekanisme memuji dan mendorong perilaku jujur, dan mekanisme kerja sama berupa insentif bersama untuk menjaga kepercayaan dan hukuman bersama untuk melanggar kepercayaan.

1. Mekanisme untuk menahan dan menghukum perilaku yang melanggar kepercayaan

Sanksi kolektif akan diterapkan pada sektor-sektor utama serta bagi pelanggar kepercayaan yang melakukan pelanggaran serius. Dalam hal ini, setiap lembaga terkait dan organisasi sosial bertanggung jawab untuk menindak serta mengevaluasi pelanggaran yang terjadi dalam lingkupnya masing-masing sesuai dengan hukum dan regulasi yang berlaku.

Selain itu, mereka juga didorong untuk berbagi informasi guna memperkuat tindakan disipliner terhadap pelanggaran kepercayaan yang bersifat berat. Beberapa contoh pelanggaran serius yang dapat dikenai sanksi mencakup tindakan yang merusak persaingan pasar yang sehat dan mengganggu tatanan sosial, seperti suap, penggelapan pajak, gagal bayar utang atau biaya layanan, penggalangan dana ilegal, penipuan kontrak, skema piramida, kegiatan usaha tanpa izin, produksi barang palsu, serta pelanggaran hak kekayaan intelektual yang disengaja. Selain itu, praktik manipulasi kualifikasi, periklanan menyesatkan, pelanggaran terhadap hak konsumen dan investor sekuritas, penyalahgunaan komunikasi digital, serta tindakan lain yang mengancam stabilitas sosial juga termasuk dalam kategori pelanggaran yang dapat dikenai sanksi ketat.

Sebagai langkah penguatan, pemerintah akan memperketat batasan administratif serta menjatuhkan sanksi bagi individu atau entitas yang terbukti melakukan pelanggaran serius. Seluruh lembaga terkait di berbagai wilayah diharuskan menjadikan para pelanggar sebagai subjek pengawasan utama dan menerapkan tindakan disipliner sesuai regulasi yang berlaku. Ini mencakup pembatasan dalam memperoleh persetujuan administratif, ketatnya pengawasan terhadap izin produksi, serta pembatasan dalam mengajukan proyek baru dan akses terhadap berbagai bentuk pendanaan, termasuk melalui pasar saham dan penerbitan obligasi. Selain itu, mereka juga dapat dilarang untuk berpartisipasi dalam lembaga keuangan, perusahaan pinjaman, penyedia jasa penjaminan keuangan, modal ventura, serta platform pembiayaan berbasis internet. Tidak hanya itu, akses terhadap layanan informasi berbasis internet juga dapat dibatasi bagi pelanggar guna mencegah risiko lebih lanjut terhadap ekosistem ekonomi dan sosial.

Kita akan memperketat regulasi pasar dan memperberat sanksi terhadap pelanggaran kepercayaan. Untuk individu maupun perusahaan yang terbukti melakukan pelanggaran serius, lembaga dan departemen terkait diwajibkan menggunakan kode kredit sosial terpadu sebagai acuan utama. Informasi yang berkaitan dengan pelanggaran tersebut harus diungkapkan secara transparan dan tepat waktu, sehingga pasar dapat mengenali potensi risiko kredit dan mencegah dampak negatif lebih lanjut. Selain itu, perusahaan serta individu yang bersangkutan akan didorong untuk memenuhi kewajiban hukum mereka. Kita juga mendukung lembaga investigasi kredit dalam mengumpulkan dan mencatat informasi mengenai pelanggaran berat ke dalam basis data serta laporan kredit. Bank komersial, lembaga sekuritas, perusahaan asuransi, dan lembaga keuangan lainnya akan diarahkan untuk menerapkan prinsip penetapan harga risiko terhadap pelanggar. Hal ini dapat dilakukan melalui peningkatan suku bunga pinjaman serta asuransi properti bagi mereka yang memiliki rekam jejak buruk dalam kredit,

atau bahkan dengan membatasi akses mereka terhadap layanan keuangan seperti pinjaman, penjaminan, asuransi, dan bentuk dukungan finansial lainnya.

Selain itu, kita juga akan memperkuat regulasi industri serta memperberat hukuman bagi pelanggaran kepercayaan dalam dunia usaha. Upaya ini mencakup penguatan kode etik profesional serta pembentukan konvensi disiplin yang lebih ketat di berbagai sektor industri guna meningkatkan transparansi dan kredibilitas ekosistem bisnis. Asosiasi industri dan kamar dagang akan didorong untuk mengembangkan sistem pencatatan dan berbagi informasi mengenai perilaku pelanggaran serius yang dilakukan oleh anggotanya. Sebagai langkah tambahan, kita mendorong kolaborasi antara asosiasi industri dengan lembaga layanan kredit pihak ketiga yang memiliki kredibilitas tinggi untuk melakukan evaluasi peringkat kredit bagi perusahaan anggotanya. Dengan mengikuti standar industri serta peraturan yang berlaku, asosiasi perdagangan dan kamar dagang akan memiliki kewenangan untuk menerapkan sanksi internal, seperti peringatan, kritik, kecaman publik, hingga penolakan keanggotaan bagi pihak-pihak yang terbukti melanggar prinsip kepercayaan dalam dunia usaha.

Kita akan memperketat pengawasan sosial serta menerapkan sanksi yang lebih tegas terhadap pelanggaran kepercayaan. Berbagai organisasi sosial akan diberdayakan untuk berperan lebih aktif dalam mengawasi dan memberikan sanksi terhadap pelanggaran kepercayaan. Selain itu, partisipasi dari sektor nonpemerintah juga akan diperluas agar dapat berkontribusi dalam upaya penegakan disiplin terhadap tindakan yang merugikan kredibilitas di masyarakat. Sebagai bagian dari langkah ini, kita akan membangun serta mengembangkan sistem pelaporan yang memungkinkan masyarakat untuk melaporkan perusahaan yang terbukti melakukan pelanggaran kepercayaan secara serius. Organisasi sosial yang relevan juga akan didorong untuk mengajukan tuntutan hukum atas kasus pelanggaran yang berdampak luas, sesuai dengan ketentuan hukum yang berlaku. Selain itu, lembaga sosial yang memiliki kredibilitas tinggi, independen, serta berorientasi pada keadilan akan diminta untuk melakukan pemantauan opini publik terhadap pelanggaran kepercayaan menggunakan teknologi big data. Hasil dari pemantauan ini akan digunakan untuk menyusun dan merilis laporan analisis kredit yang mencakup aspek regional maupun industri tertentu. Kita juga akan memperketat sistem pencatatan kredit individu serta mendorong penerapan kebijakan yang memungkinkan sanksi lebih efektif terhadap individu yang bertanggung jawab atas pelanggaran kepercayaan. Jika sebuah perusahaan atau lembaga publik melakukan pelanggaran serius, catatan tersebut akan dimasukkan ke dalam riwayat kredit pribadi dari perwakilan hukum, penanggung jawab utama, serta individu lain yang memiliki tanggung jawab langsung. Saat menerapkan sanksi kepada perusahaan dan institusi yang melanggar kepercayaan, hukuman yang sesuai juga akan

diberlakukan terhadap pihak yang bertanggung jawab sesuai dengan peraturan hukum dan kebijakan yang berlaku. Dengan membangun basis data catatan kredit pribadi yang terintegrasi serta menerapkan mekanisme sanksi yang lebih ketat, kita dapat memastikan bahwa tindakan disipliner terhadap pelanggaran kepercayaan tidak hanya diterapkan pada entitas bisnis, tetapi juga pada individu yang terlibat langsung dalam pelanggaran tersebut.

2. Mekanisme untuk memuji dan mendorong perilaku jujur

Kita akan mengembangkan model integritas melalui berbagai saluran dengan melibatkan departemen terkait serta organisasi sosial. Setiap entitas akan didorong untuk mencatat riwayat kredit subjek yang berada dalam pengawasan serta layanan mereka. Selain itu, individu maupun perusahaan yang memiliki rekam jejak kredit yang baik akan dipromosikan sebagai contoh bagi masyarakat. Dengan bekerja sama dengan berbagai pihak, kita dapat menciptakan sistem insentif yang mendorong perilaku terpercaya. Di sisi lain, organisasi industri juga akan didorong untuk meningkatkan mekanisme evaluasi kredit bagi anggotanya. Perusahaan juga akan dipandu untuk secara proaktif merilis komitmen terkait kredibilitas mereka, baik dalam aspek kualitas produk, layanan, maupun standar operasional lainnya. Mereka juga didorong untuk membuat pernyataan terbuka terkait standar yang diterapkan serta berpartisipasi dalam pengawasan sosial. Langkah ini bertujuan untuk menciptakan lingkungan bisnis yang sehat, di mana perusahaan berlomba-lomba menjadi model integritas.

Selain itu, kita akan mengeksplorasi penerapan sistem “jalur hijau” dalam proses perizinan administratif. Perusahaan yang memiliki riwayat kredit bersih selama tiga tahun berturut-turut akan mendapatkan kemudahan dalam pengurusan perizinan, seperti percepatan pemrosesan dokumen atau penerimaan berkas meskipun belum sepenuhnya lengkap, dengan syarat mereka berkomitmen untuk melengkapinya dalam batas waktu yang ditentukan.

Dalam upaya meningkatkan pelayanan publik, pemerintah akan mengutamakan pelaku usaha yang memiliki rekam jejak kejujuran dalam penerapan berbagai kebijakan insentif, seperti dukungan dana fiskal serta program investasi. Selain itu, individu yang memiliki reputasi baik akan mendapatkan prioritas dalam berbagai sektor, termasuk pendidikan, ketenagakerjaan, kewirausahaan, serta jaminan sosial. Dalam transaksi yang melibatkan sumber daya publik, entitas bisnis yang terpercaya akan diberikan poin tambahan dalam sistem evaluasi, sesuai dengan regulasi yang berlaku.

Pengawasan administratif terhadap perusahaan yang telah terbukti memiliki kredibilitas tinggi juga akan disesuaikan untuk memberikan fleksibilitas lebih besar. Otoritas pasar di semua tingkat akan memanfaatkan teknologi big data dalam mengelola regulasi, dengan mengklasifikasikan perusahaan berdasarkan rekam jejak kredit mereka. Perusahaan yang

memiliki reputasi baik akan diberikan kemudahan dalam proses pengawasan serta layanan administratif yang lebih efisien.

Di samping itu, kita akan berupaya menurunkan biaya transaksi di pasar dengan mendorong departemen serta unit terkait untuk mengembangkan program insentif kredit. Lembaga keuangan, platform penjualan, dan penyedia layanan pasar akan didorong untuk menggunakan informasi kredit sebagai dasar dalam memberikan perlakuan istimewa kepada pelaku usaha yang memiliki reputasi baik, sehingga mereka dapat memperoleh lebih banyak kesempatan serta manfaat dalam ekosistem bisnis.

Untuk meningkatkan apresiasi terhadap entitas pasar yang jujur, informasi kredit positif dari para pelaku usaha akan dipublikasikan secara berkala melalui situs web pemerintah maupun platform "Credit China." Hal ini bertujuan agar kepercayaan menjadi faktor utama dalam alokasi sumber daya di pasar. Lembaga investigasi kredit juga akan didorong untuk meningkatkan pengumpulan data positif dari berbagai entitas bisnis guna menyeimbangkan sistem penilaian, terutama dalam industri yang memiliki tantangan terkait kepercayaan. Selain itu, asosiasi industri serta kamar dagang akan didorong untuk memperkuat budaya integritas dalam sektor mereka, dengan menegakkan disiplin serta memberikan penghargaan bagi anggotanya yang memiliki catatan kredit yang baik. Dengan cara ini, kita dapat membangun ekosistem bisnis yang lebih sehat dan berbasis kepercayaan, di mana perusahaan yang jujur mendapatkan lebih banyak manfaat serta pengakuan dalam pasar.

3. Membangun mekanisme kerja sama untuk insentif bersama bagi pihak yang menjaga kepercayaan dan sanksi bersama bagi pihak yang melanggar kepercayaan.

Kita akan menerapkan mekanisme umpan balik yang efektif untuk menjaga sistem integritas dengan menetapkan prosedur insentif dan sanksi yang terkoordinasi antar kementerian dalam pembangunan sistem kredit sosial. Mekanisme ini memungkinkan adanya tindakan bersama dalam memberikan penghargaan kepada individu atau entitas yang menjaga kepercayaan serta memberikan sanksi bagi mereka yang melakukan pelanggaran. Setiap departemen yang terlibat bertanggung jawab dalam menentukan subjek yang berhak menerima insentif maupun sanksi, sementara eksekusi tindakan akan dilaksanakan oleh instansi pelaksana yang telah ditunjuk.

Selain itu, sistem koordinasi antara kementerian dan provinsi juga akan diperkuat, memungkinkan adanya kerja sama lintas daerah dalam menerapkan kebijakan insentif dan sanksi kredit. Pemerintah daerah didorong untuk mengambil langkah aktif dalam mengidentifikasi subjek yang patuh maupun yang melanggar aturan di wilayah masing-masing serta membangun sistem berbagi informasi kredit yang lebih efisien antar sektor. Dengan

demikian, sistem ini dapat mendorong transparansi serta meningkatkan koordinasi antar wilayah dalam hal pengawasan dan evaluasi kredit.

Dalam mendukung transparansi, kita juga akan meningkatkan sistem publikasi informasi kredit, di mana pemerintah daerah serta instansi terkait diwajibkan untuk mempublikasikan informasi terkait lisensi administratif dan sanksi yang diberikan kepada individu, badan hukum, maupun organisasi lain. Informasi ini harus tersedia secara daring dalam waktu tujuh hari kerja serta dikumpulkan dalam platform "Credit China" untuk memudahkan akses publik. Pengadilan juga diharapkan turut berkontribusi dengan mempublikasikan keputusan hukum serta daftar individu atau entitas yang memiliki catatan pelanggaran kepercayaan.

Untuk mempercepat pengumpulan dan distribusi informasi kredit, platform berbagi data nasional akan dikembangkan guna mengintegrasikan data dari berbagai sektor dan wilayah. Sistem ini akan berfungsi sebagai pusat pengelolaan informasi kredit yang memungkinkan adanya koordinasi otomatis dalam hal pemantauan kredit, pemberian insentif, serta penegakan sanksi. Integrasi data juga akan diperluas dengan melibatkan lembaga keuangan, asosiasi perdagangan, dan organisasi lainnya agar sistem insentif dan sanksi kredit dapat diterapkan secara lebih luas dan efektif.

Sistem daftar merah dan daftar hitam kredit juga akan ditingkatkan, memastikan bahwa prosedur pencatatan serta penghapusan entitas dari daftar tersebut dilakukan secara transparan dan sesuai regulasi. Lembaga keuangan, badan pemeringkat, serta asosiasi industri akan dilibatkan dalam penyusunan daftar ini agar dapat menjadi referensi yang kredibel bagi pemerintah dalam menetapkan kebijakan kredit. Dengan sistem ini, entitas yang memiliki reputasi baik dapat mendapatkan berbagai keuntungan, sementara yang memiliki catatan buruk akan dikenai pembatasan tertentu.

Selain itu, kami akan membangun sistem insentif dan disipliner yang jelas, dengan membagi tindakan menjadi dua kategori utama: pertama, tindakan yang bersifat wajib dan harus diterapkan sesuai hukum; dan kedua, tindakan rekomendasi yang dapat diterapkan oleh berbagai wilayah dan departemen sesuai dengan kebijakan yang berlaku. Mekanisme perbaikan kredit juga akan ditetapkan untuk memberikan kesempatan bagi individu atau entitas yang telah melakukan pelanggaran guna memperbaiki reputasi mereka dalam jangka waktu tertentu. Jika mereka berhasil menghilangkan dampak negatif dari pelanggaran tersebut, maka sanksi yang diterapkan sebelumnya dapat dicabut.

Sebagai bentuk perlindungan hak-hak individu dan entitas bisnis, sistem keberatan dan pengaduan terkait informasi kredit akan diperkuat. Jika ada kesalahan dalam pencatatan atau penerapan sanksi yang dianggap merugikan, subjek terkait berhak mengajukan keberatan, yang

kemudian akan diverifikasi oleh penyedia informasi. Jika terbukti ada kesalahan, data tersebut harus segera diperbaiki atau dihapus. Jika sanksi yang dijatuhkan terbukti merugikan hak-hak sah subjek yang bersangkutan, maka instansi terkait wajib mengambil langkah pemulihan untuk mengembalikan kredibilitas mereka.

Untuk memastikan efektivitas sistem ini, mekanisme pelacakan dan pemantauan akan diterapkan guna mengawasi pelaksanaan insentif dan sanksi kredit secara menyeluruh. Platform berbagi informasi kredit nasional akan dimanfaatkan secara optimal untuk mencatat, memonitor, serta mengevaluasi implementasi kebijakan ini. Selain itu, sistem pengawasan dan penilaian akan dibangun untuk memastikan bahwa setiap kebijakan yang diterapkan benar-benar memberikan dampak positif dalam membangun ekosistem bisnis yang berbasis integritas dan kepercayaan.

7.3.3 Peraturan, Sistem, dan Pembangunan Integritas

Penerapan hukum dan peraturan yang kuat, serta pembentukan budaya integritas, menjadi faktor krusial dalam mengelola risiko kredit dalam perdagangan elektronik. Langkah pertama yang perlu dilakukan adalah memperbaiki regulasi yang ada dengan mendorong pengumpulan, berbagi, serta pemanfaatan informasi kredit secara lebih transparan, sekaligus memperketat sanksi bagi pelanggar kepercayaan. Sejalan dengan upaya memperkuat pengawasan kredit dan koordinasi antarinstansi, setiap wilayah dan departemen diharapkan dapat mengusulkan revisi atau menyusun amandemen terhadap undang-undang, peraturan, serta pedoman yang relevan guna memastikan efektivitas penerapannya. Selain itu, diperlukan penetapan serta penyempurnaan standar dan norma terkait manajemen kredit. Hal ini mencakup perumusan pedoman dalam proses pengumpulan, penyimpanan, berbagi, serta evaluasi informasi kredit, termasuk klasifikasi berdasarkan tingkat risiko. Standarisasi juga perlu diterapkan dalam pembangunan platform berbagi data kredit di berbagai tingkatan, dengan menyatukan format dan antarmuka data agar sistem dapat terintegrasi secara optimal. Setiap daerah dan instansi harus menyesuaikan prosedur operasional sesuai dengan kondisi spesifik mereka, sehingga regulasi terkait dapat diimplementasikan dengan lebih efisien. Selain aspek hukum dan teknis, membangun budaya integritas juga menjadi bagian penting dalam upaya ini. Langkah konkret yang dapat diambil adalah dengan menyelenggarakan program edukasi yang melibatkan berbagai elemen masyarakat untuk menanamkan kesadaran akan pentingnya menjalankan bisnis dengan itikad baik sesuai aturan yang berlaku. Kampanye ini bertujuan untuk menanamkan pemahaman bahwa integritas bukan hanya kewajiban hukum, tetapi juga faktor yang dapat meningkatkan reputasi dan kelangsungan usaha. Lebih lanjut,

mekanisme pengawasan berbasis opini publik juga harus diperkuat dengan memanfaatkan berbagai saluran media, seperti pers, radio, televisi, internet, dan platform digital lainnya. Dengan mempublikasikan kasus pelanggaran kepercayaan yang berdampak luas dan memiliki konsekuensi serius, diharapkan dapat muncul tekanan sosial serta kendala moral yang membuat individu atau perusahaan lebih berhati-hati dalam bertindak. Di sisi lain, bagi individu atau entitas yang pernah melakukan pelanggaran kepercayaan, perlu disediakan mekanisme bimbingan dan bantuan agar mereka dapat memperbaiki reputasi dan kembali beroperasi dengan lebih bertanggung jawab. Pendekatan ini bertujuan untuk menciptakan keseimbangan antara penegakan hukum dan kesempatan bagi pelanggar untuk memperbaiki diri, sehingga sistem kredit yang diterapkan dapat berjalan secara lebih adil dan berkelanjutan.

BAB 8
Mengendalikan Risiko Personel Ecommerce Pembangunan

Dan penerapan personel khusus sangat penting untuk pengembangan e-commerce. Mereka tidak hanya merupakan komponen penting dalam pembuatan dan implementasi sistem e-commerce, tetapi mereka juga merupakan subjek manajemen risiko e-commerce. Manajemen risiko personel e-commerce adalah komponen penting dalam manajemen keamanan e-commerce.

8.1 Analisis Risiko Personel E-commerce

E-commerce memiliki banyak pengetahuan. Orang-orang yang bekerja dalam perdagangan elektronik biasanya diharuskan tidak hanya memiliki keterampilan dan pengetahuan bisnis tertentu, tetapi juga memiliki keterampilan dan pengetahuan dalam teknologi informasi. Kejahatan dunia maya yang menggunakan informasi e-commerce sangat berhati-hati dalam hal intelijen dan penyembunyian, dan bahkan seorang karyawan biasa dapat menyebabkan kerugian besar atau konsekuensi bencana bagi perusahaan perdagangan elektronik. Akibatnya, keselamatan karyawan sangat penting untuk keamanan e-commerce.

8.1.1 Perlunya Manajemen Risiko untuk Personel Ecommerce

Dalam e-commerce, risiko personel mengacu pada ketidakpastian perilaku yang tidak disengaja atau disengaja dari para praktisi e-commerce. Risiko personel biasanya berasal dari aspek internal dan eksternal perusahaan e-commerce. Dengan peningkatan mekanisme keamanan informasi perusahaan e-commerce, semakin sulit bagi pihak luar untuk memanfaatkan kerentanan atau cacat keamanan sistem untuk memasuki sistem target. Sebaliknya, ancaman dari perusahaan e-commerce internal berasal dari sumber yang sama. Saat ini, ada banyak masalah yang dihadapi oleh manajemen personalia perusahaan e-commerce, di antaranya adalah: Pertama, manajemen risiko personel e-commerce tidak mendapat perhatian yang memadai. Manajer bisnis e-commerce biasanya fokus pada sistem, jaringan, informasi dan data, transaksi, dan sebagainya, tetapi seringkali mengabaikan manajemen risiko personel. Bisnis e-commerce akan mengalami kerugian yang lebih besar saat terjadi risiko personalia. Kedua, ancaman keamanan terbesar bagi perusahaan e-commerce berasal dari risiko personalia. Ini karena, berbeda dengan ancaman keamanan eksternal, ancaman keamanan internal berasal dari personel internal perusahaan e-commerce, sehingga sulit untuk dideteksi dan dicegah, dan kerugian juga lebih besar. Untuk personel e-commerce, manajemen risiko sangat penting. Pertama-tama, manajemen risiko personalia sangat penting untuk perusahaan e-commerce. Salah satu sumber daya terpenting perusahaan adalah

karyawan. Setiap tahap perkembangan bisnis e-commerce melibatkan risiko personalia. Di industri e-commerce, persaingan untuk mendapatkan talenta sangat ketat. Namun, sistem manajemen risiko personalia yang baik dapat membantu perusahaan untuk mempertahankan, menarik, dan memotivasi karyawan mereka, serta mengurangi berbagai risiko yang ditimbulkan oleh karyawan. Perusahaan e-commerce dapat berhasil di pasar jika mereka dapat mengendalikan risiko penunjukan dan manajemen personalia. Salah satu bahaya yang paling signifikan dalam e-commerce adalah risiko personalia, yang merupakan komponen penting dari manajemen risiko perusahaan e-commerce. Kedua, strategi perusahaan e-commerce dibantu oleh manajemen risiko personalia. Semua anggota departemen harus bekerja sama untuk mencapai strategi e-commerce, jadi karyawan adalah kuncinya. Oleh karena itu, pengendalian risiko personel yang baik dapat sangat mengurangi dampak negatif personel terhadap perusahaan dan membantu strategi bisnis e-commerce berjalan.

8.1.2 Penyebab Risiko dan Jenis Personel E-commerce

1. Analisis penyebab risiko personel e-commerce

Ada banyak alasan untuk menganggap staf e-commerce berbahaya. Pertama dan terpenting, terlalu bergantung pada teknologi keamanan. Manajer dalam manajemen yang sebenarnya sering menganggap teknologi keamanan sebagai bagian dari manajemen keamanan secara keseluruhan, tetapi ini tidak selalu benar. Pertama dan terpenting, banyak teknologi keamanan hanya dikembangkan setelah terjadi ancaman keamanan. Manajer yang terlalu bergantung pada sistem teknis adalah pasif dalam manajemen. Kedua, karena manajemen keselamatan adalah proses yang berkelanjutan, teknologi keselamatan hanya dapat digunakan oleh orang-orang dan dapat memainkan peran terbesar dalam manajemen yang efektif. Untuk menjamin keamanan e-commerce, kombinasi perlindungan personel dan teknologi keselamatan lebih baik. Kedua, sistem manajemen personalia tidak lengkap. Setiap tahap manajemen personalia internal (termasuk perekrutan, penilaian, pemecatan, dll.) tidak memiliki sistem yang relevan, yang menunjukkan ketidaksempurnaan sistem manajemen personalia. Pada saat yang sama, sistem manajemen personalia mitra juga melakukan hal yang sama. Cara penting bagi perusahaan e-commerce untuk menerapkan manajemen keamanan adalah dengan menyewa layanan keamanan. Dalam bisnis e-commerce, outsourcing layanan keamanan dilakukan untuk menutupi kekurangan sumber daya manusia atau kemampuan teknis manajemen keamanan perusahaan dengan bantuan lembaga profesional pihak ketiga. Namun, ada sistem manajemen keselamatan yang tidak sempurna dalam hal manajemen personalia koperasi. Misalnya, mereka tidak melakukan analisis menyeluruh tentang tujuan implementasi layanan outsourcing,

strategi implementasi, sumber daya manusia, persyaratan tingkat keamanan, dan lainnya. Akibatnya, prosedur serah terima pekerjaan tidak standar dan prosedur yang relevan tidak sempurna. Ketiga, pendidikan dan pelatihan keselamatan tidak ada. Beberapa perusahaan e-commerce berfokus pada pelatihan keterampilan personel, tetapi kurangnya pendidikan dan pelatihan tentang keamanan, kesadaran keselamatan, kesadaran kerahasiaan, sistem kerahasiaan, dan manajemen perusahaan. Sistem pendidikan dan pelatihan keselamatan dan desain kurikulum yang tidak masuk akal membuat pendidikan dan pelatihan keselamatan tidak efektif.

2. Jenis risiko personel e-commerce

Risiko personalia e-commerce dapat dibagi menjadi risiko personalia internal dan eksternal, menurut berbagai sumber. Dalam industri e-commerce, risiko personel internal mengacu pada bahaya yang ditimbulkan oleh karyawan internal perusahaan. Dari sudut pandang manajemen keamanan, sangat penting untuk menerapkan kontrol otoritas untuk pengawas sumber daya manusia dan personel teknis di perusahaan e-commerce. Perusahaan e-commerce harus melakukan yang terbaik untuk mengurangi risiko yang ditimbulkan oleh staf internal. Manajer bisnis e-commerce harus mempertimbangkan risiko yang datang dari karyawan internal. Ini karena personel internal sering dapat mengakses sistem perusahaan dan penyimpanan informasi penting, proses pemrosesan, dan aturan dan peraturan internal. Akibatnya, serangan terhadap sistem ini memiliki tingkat keberhasilan yang tinggi dan dapat menyebabkan kerusakan. Personel internal non-perusahaan, yang mencakup mereka yang bekerja sama dengan perusahaan atau memiliki hubungan lain dengan perusahaan, seperti hubungan layanan, hubungan kompetitif, atau bahkan tidak memiliki hubungan dengan perusahaan, dianggap memiliki risiko personel eksternal. Personel yang bekerja sama dengan perusahaan biasanya memiliki hubungan dekat dengan perusahaan karena kebutuhan. Ada ancaman keamanan jika perusahaan secara tidak tepat mengelola otoritas personel tersebut. Dua jenis karyawan luar lainnya dapat memanfaatkan teknologi ultra-tinggi atau kenyamanan kerja mereka untuk memanfaatkan cacat dan kerentanan sistem untuk mencuri data atau melancarkan serangan, yang menempatkan perusahaan e-commerce di bahaya.

8.2 Identifikasi, Penilaian, dan Pengambilan Keputusan Personel E-commerce

Salah satu risiko keamanan terbesar bagi karyawan e-commerce adalah risiko personel internal. Oleh karena itu, bagian ini terutama menganalisis cara mengidentifikasi, menilai, dan membuat keputusan tentang pengendalian risiko personel internal di perusahaan e-commerce.

8.2.1 Identifikasi Risiko Personel E-commerce

Semua karyawan perusahaan e-commerce menghadapi risiko sebelum mulai bekerja, selama masa kerja, dan selama proses pemutusan hubungan kerja. Risiko sebelum perekrutan terutama mencakup asimetri informasi dan prosedur yang tidak tepat untuk menerima karyawan. Untuk mendapatkan pekerjaan, kandidat mungkin mengambil berbagai cara untuk memberikan informasi yang salah kepada perusahaan, yang memengaruhi penilaian kandidat dan membuat kandidat yang tidak memiliki kualitas dan kemampuan yang diperlukan untuk posisi yang sebenarnya. Selain itu, proses rekrutmen yang tidak masuk akal akan berdampak pada hasil rekrutmen yang tidak adil dan tidak masuk akal. Proses penerimaan karyawan yang buruk Misalnya, karyawan seringkali tidak memeriksa laporan kredit mereka sebelum bekerja di perusahaan, yang meningkatkan risiko pekerjaan perusahaan karena mereka memiliki masalah kredit. Dalam bidang ketenagakerjaan, yang paling umum adalah risiko manajemen kinerja, manajemen gaji, dan pelatihan karyawan. Risiko manajemen kinerja dapat berasal dari berbagai sumber, seperti sistem manajemen kinerja yang tidak berfungsi dengan baik, kebijakan dan metode penilaian kinerja yang tidak sesuai, indeks penilaian kinerja yang tidak dirancang dengan baik, atau penilaian kinerja tidak mencapai tujuan yang diharapkan. Risiko pengelolaan kompensasi terutama tercermin dari masalah yang disebabkan oleh perhitungan, persetujuan, dan pembayaran kompensasi yang tidak wajar, serta perumusan kebijakan kompensasi yang tidak wajar. Masalah seperti perhitungan gaji yang salah, perhitungan yang salah atau perhitungan ganda, klaim kompensasi yang salah, pelaporan upah lembur yang berlebihan, dan situasi lainnya dapat muncul sebagai akibat dari manajemen yang buruk dan pembagian tanggung jawab yang tidak jelas. Rencana pelatihan karyawan yang tidak masuk akal dan tidak melakukan penyelidikan dan analisis kebutuhan pelatihan sebelum pelatihan karyawan menyebabkan tujuan dan objek pelatihan yang tidak jelas, pengaturan pelatihan yang tidak tepat, waktu pelatihan yang tidak masuk akal, siklus, dan konten situasi aktual, yang menyebabkan implementasi pelatihan yang buruk atau efek yang buruk.

Pengungkapan rahasia perusahaan, lowongan pekerjaan, pembalasan, dll. adalah risiko utama setelah pemutusan hubungan kerja. Pertama, manajer dan staf teknis di posisi kunci perusahaan e-commerce menguasai teknologi dan informasi penting perusahaan, dan jika mereka meninggalkan kantor, mereka berisiko membocorkannya. Kedua, jika staf manajemen pos utama dan staf teknis pergi, akan ada kekosongan pekerjaan, yang menghambat kemajuan normal pekerjaan. Yang lain adalah melawan tujuan Anda. Ketidakpuasan karyawan selama pekerjaan mereka, tindakan balas dendam setelah diberhentikan, dan perilaku yang merugikan perusahaan dikenal sebagai tindakan ambisi.

8.2.2 Penilaian Risiko untuk Personel E-commerce

Komponen utama penilaian risiko personel e-commerce adalah proses dan indeks penilaian risiko personel.

Pertama, indikator penilaian risiko personel e-commerce. Ini termasuk indeks evaluasi pribadi, indeks tingkat kecocokan karyawan dengan perusahaan, dan indeks keamanan karyawan.

Indikator untuk evaluasi pribadi adalah sebagai berikut: indikator kualitas moral termasuk kualitas pemikiran keselamatan, integritas keselamatan, etika profesional, dan konsep keselamatan; indikator kualitas profesional termasuk latar belakang pendidikan, pengalaman praktis, sistem pengetahuan dan keterampilan; indikator kualitas fisik termasuk kualitas perhatian, karakteristik reaksi, dan kemampuan fisik; indikator kualitas psikologis termasuk stres psiko-logis, stres emosional, kejenuhan kerja, dan stres fisik; dan indikator kualitas psikologis termasuk stres

Tingkat kecocokan personel dan perusahaan terdiri dari: kemampuan karyawan dan jenis pekerjaan, persyaratan kemampuan kerja yang berbeda, dan upaya untuk mendorong kinerja mereka; kepuasan kerja karyawan, yang dapat mencakup kompensasi, perlakuan, penghargaan, dan kesempatan untuk berkembang; identitas karyawan, pengenalan gaya manajemen perusahaan, budaya perusahaan, hubungan antarpribadi, keadilan, komunikasi yang lancar, dll.

Indikator jaminan keselamatan karyawan: Indeks jaminan pendidikan dan pelatihan keselamatan karyawan menunjukkan bagaimana pendidikan dan pelatihan keselamatan karyawan dilakukan. Perusahaan harus membuat dan menerapkan rencana pendidikan dan pelatihan keselamatan karyawan sesuai dengan peraturan dan persyaratan jabatan, dan memberikan sumber daya yang sesuai untuk melakukannya. Indeks jaminan keselamatan produksi termasuk ma Sehubungan dengan manajemen kesehatan kerja, perusahaan e-commerce harus mematuhi peraturan, peraturan, standar, dan norma yang berlaku. Mereka juga harus memastikan bahwa karyawan berada dalam lingkungan kerja yang aman, dengan fasilitas dan peralatan yang sesuai untuk menjaga kesehatan mereka, dan melakukan inspeksi dan perlindungan keselamatan yang sesuai.

Kedua, proses penilaian risiko personel e-commerce. Proses ini terutama mencakup identifikasi risiko, analisis risiko, pengambilan keputusan tentang pengendalian risiko, dan implementasi pengendalian risiko, yang merupakan siklus dan proses optimalisasi yang berkelanjutan.

Identifikasi Risiko: Cari dan temukan sumber risiko dengan melakukan penelitian yang ditargetkan pada perekrut, staf yang bertugas, staf yang mengalami perubahan atau pemecatan, staf yang bekerja sama, dan staf yang bersaing.

Analisis risiko: Hasil survei risiko dan pengalaman digunakan untuk memprediksi kemungkinan terjadinya risiko. Kemungkinan terjadinya risiko dapat diwakili dengan persentase, dan kelompok prioritas dapat ditetapkan berdasarkan kemungkinan terjadinya risiko.

memungkinkan risiko. Keputusan pengendalian risiko: Hasil analisis risiko, seperti yang dijelaskan di Bagian 8.2.3, menentukan keputusan pengendalian risiko.

Implementasi pengendalian risiko: Keputusan pengendalian risiko menetapkan bahwa draf rencana implementasi pengendalian risiko harus dibuat dan diserahkan kepada personel terkait untuk dibahas. Rencana harus diterapkan setelah disetujui oleh atasan. Setelah skema diterapkan dalam jangka waktu tertentu, risiko dievaluasi, masalah yang muncul saat diterapkan dianalisis, pengalaman dirangkum, dan skema dioptimalkan.

8.2.3 Keputusan Pengendalian Risiko Personel E-commerce

Perusahaan e-commerce harus mengikuti beberapa prinsip ketika membuat keputusan pengendalian risiko personalia. Pertama, prinsip kewajaran, kewajaran, dan keadilan. Berdasarkan hasil penilaian risiko personalia, manajer harus mengikuti prinsip kewajaran dan keadilan saat membuat keputusan pengendalian risiko untuk menghindari prasangka dan rasa suka dan tidak suka pribadi, terutama keluhan pribadi. Prinsip kedua adalah rasionalitas dan legalitas. Berdasarkan hasil penilaian risiko personalia, manajer harus mengikuti prinsip kewajaran. Menurut hasil analisis risiko personel, perusahaan e-commerce membuat berbagai jenis keputusan pengendalian risiko.

Pelatihan dan Pendidikan Berkelanjutan: Pengetahuan, teknologi, dan gagasan baru terus muncul seiring perkembangan masyarakat. Sistem pengetahuan dan kemampuan karyawan juga perlu diperkuat dan diperbarui. Perusahaan harus memberikan karyawan saat ini pelatihan yang tepat dan kesempatan pendidikan yang berkelanjutan. Manajer harus merencanakan, mengatur, dan mengimplementasikan secara efisien untuk memastikan bahwa kemampuan karyawan dan kebutuhan pekerjaan tetap sesuai dalam perkembangan yang terus berubah.

perkembangan yang terus berubah. Pemindahan posisi: Karyawan harus disesuaikan ke pekerjaan yang lebih sesuai jika kemampuan kerja mereka tidak cocok dengan pekerjaan yang

ada, mereka tidak kompeten untuk pekerjaan yang ada, atau kemampuan mereka melebihi persyaratan pekerjaan.

Kritik dan penghargaan: Kritik dan penghargaan adalah cara yang baik bagi perusahaan untuk menerapkan manajemen keselamatan; kritik juga memiliki peran penguatan. Penghargaan membantu karyawan, tidak hanya meningkatkan rasa pencapaian mereka dan mendorong mereka untuk mempertahankan reputasi mereka, tetapi juga membantu menciptakan suasana kerja yang kompetitif dan mendorong kemajuan. Sebaliknya, hukuman dapat berfungsi sebagai sarana pencegahan dan pengingatkan, membuat karyawan berperilaku buruk. Melakukan penghargaan dan hukuman yang jelas dan menjelaskan pekerjaan dan kekurangan. Namun, tidak mudah untuk membuat "hadiah" dan "hukuman" benar-benar memobilisasi semangat dan kesadaran keselamatan di antara manajer dan karyawan. Oleh karena itu, kita harus mempertimbangkan bagaimana dan bagaimana kritik dan penghargaan dilakukan. Salah satunya adalah dengan memuji, pujian, dan kombinasi yang sesuai; ini lebih sesuai dengan prinsip psikologi karena pujian dapat membuat orang yang dipuji memiliki suasana hati yang positif, membuat mereka merasa bahagia, dan kemudian menjadi bersemangat, menghadapi masalah keselamatan, dan menjadikan perilaku keselamatan sebagai perilaku yang disadari. Yang kedua adalah mempertimbangkan alasan pujian, kritik, penghargaan, dan hukuman. Kritik dan hukuman dimaksudkan untuk menunjukkan perilaku yang kurang atau tidak diharapkan. Misalnya, pemimpin perusahaan harus secara sadar mengatasi masalah "disiplin tenaga kerja", memuji yang baik dan mengecam yang buruk, untuk menciptakan keadaan disiplin yang diharapkan. Ketiga, ini bervariasi dari individu ke individu dan memiliki berbagai bentuk. Kami harus mempertimbangkan psikologi karyawan yang berbeda saat menggunakan hadiah dan hukuman untuk memberikan insentif. Kami juga harus mempertimbangkan berbagai metode dan persyaratan. Karena masing-masing pekerja memiliki karakteristik unik, mereka merespons penguatan positif dan negatif dengan cara yang berbeda. Kita harus memperhatikan perbedaan psikologis karyawan untuk mencapai efek penguatan yang baik.

Penurunan pangkat: Jika karyawan melanggar sistem atau peraturan perusahaan yang relevan, menyebabkan kerugian atau dampak tertentu pada perusahaan, atau sebagai orang yang bertanggung jawab atau peserta dalam acara tersebut, perusahaan harus menskorsnya selama penyelidikan.

Pemecatan: Jika seorang karyawan melanggar hukum dan peraturan nasional atau sistem atau peraturan perusahaan yang relevan dan menyebabkan kerugian atau dampak yang

signifikan terhadap perusahaan, perusahaan harus menghentikan atau mengakhiri kontrak kerjanya dan mengikuti peraturan nasional.

Mengusir: Jika karyawan melanggar hukum dan peraturan nasional atau sistem atau peraturan perusahaan yang relevan dan menyebabkan kerugian atau dampak yang signifikan pada perusahaan, perusahaan harus mengeluarkannya dari pekerjaan.

Selain itu, perusahaan juga harus meningkatkan sistem manajemen perusahaan relevan,memperkuat pembangunan budaya perusahaan, sehingga dapat mengurangi risiko personel.

8.3 Implementasi Pengendalian Risiko untuk Personel E-commerce

Pengendalian risiko personel e-commerce mengacu pada penggunaan berbagai metode pengendalian risiko untuk mengelola risiko yang dihadapi oleh individu yang terlibat dalam topik ini. Setiap tindakan yang dilakukan oleh karyawan perusahaan harus mematuhi hukum, peraturan, dan regulasi perusahaan, dan menghindari tindakan ilegal dan kriminal serta informasi berbahaya. Perusahaan e-commerce harus mengambil tindakan yang efektif untuk mengendalikan risiko personel.

8.3.1 Sistem Manajemen Personalia

Perusahaan e-commerce terutama melakukan pengendalian risiko melalui sistem manajemen otorisasi dan perekrutan karyawan.

1. Sistem ketenagakerjaan personalia

Untuk mengurangi dampak negatif dari elemen personalia terhadap keselamatan bisnis e-commerce, perusahaan e-commerce harus membuat dan menerapkan sistem ketenagakerjaan yang masuk akal. Dalam sistem ketenagakerjaan, harus ada tiga tahap: sebelum perekrutan, selama perekrutan, dan pemutusan hubungan kerja. Sebelum dipekerjakan, kandidat dievaluasi. Personel manajemen, personel jabatan tetap, personel sementara, dll. termasuk dalam daftar peninjauan. Informasi latar belakang personel, kesadaran keselamatan, kesadaran hukum, dan keterampilan keamanan adalah bagian dari peninjauan. Selama peninjauan latar belakang personel, semua hukum yang terkait dengan privasi pribadi, perlindungan data, dan penunjukan harus diperhatikan. Selain itu, materi rekomendasi yang efektif (misalnya, perusahaan dan dokumen yang ditulis oleh individu), resume kandidat yang akan dipekerjakan (misalnya, resume yang lengkap dan akurat), kompetensi profesional, identitas pribadi (misalnya, paspor atau dokumen serupa), dan rincian tambahan (misalnya, catatan kredit atau catatan kriminal) harus dipertimbangkan jika diizinkan.

Perusahaan harus memastikan bahwa karyawannya memenuhi standar yang sesuai. Dalam penilaian karyawan, standar penilaian harus disesuaikan dengan tingkat keselamatan yang ditetapkan oleh sistem manajemen keselamatan. Saat menentukan peran penting dalam sistem manajemen keselamatan, seperti supervisor keselamatan, administrator keselamatan, teknisi keselamatan, dan personel keselamatan, perusahaan harus melakukan penilaian menyeluruh dan menilai kapasitas perusahaan mereka. Perusahaan harus memastikan apakah orang yang akan dipekerjakan memiliki kemampuan yang diperlukan untuk memainkan peran keamanan, terutama jika peran tersebut penting bagi perusahaan. Perusahaan harus melakukan verifikasi yang lebih rinci jika posisi yang sesuai dengan kandidat memiliki hak untuk mengakses fasilitas pemrosesan informasi, terutama untuk memproses informasi keuangan atau rahasia. Selain itu, perjanjian yang ditandatangani oleh perusahaan dan mitra harus mengatur tanggung jawab tinjauan. Tentu saja, perusahaan harus mengumpulkan dan memproses informasi dari semua karyawan sesuai dengan hukum yang berlaku, serta memberi tahu karyawan terlebih dahulu sebelum peninjauan dimulai.

Perusahaan harus membuat rencana pemilihan personel. Ketika perusahaan memilih karyawan tertentu, mereka harus mempertimbangkan prinsip evaluasi dan masa percobaan sebelum memulai pekerjaan. Semua anggota staf harus mematuhi prinsip "hak istimewa minimum" dan memikul tanggung jawab dan kerahasiaan yang terkait. Kontrak yang ditandatangani dengan karyawan harus menunjukkan bahwa perusahaan bertanggung jawab atas keamanan informasi karyawannya. Pertama, persyaratan dan ketentuan, termasuk perjanjian kerahasiaan atau kerahasiaan sebelum mendapatkan akses ke fasilitas pemrosesan informasi; tanggung jawab hukum dan hak-hak karyawan; tanggung jawab untuk mengelola aset, fasilitas pemrosesan, dan layanan yang terkait dengan informasi; tanggung jawab untuk menangani informasi yang dikirim ke pihak lain; dan tindakan terhadap karyawan yang tidak mematuhi peraturan keamanan perusahaan. Perlu diingat bahwa kewajiban yang tercantum dalam syarat dan ketentuan pekerjaan harus dipertahankan untuk jangka waktu tertentu setelah karyawan dipecat. Kedua, kode: Perusahaan harus membuat kode etik yang menjelaskan tanggung jawab karyawan terhadap kerahasiaan, perlindungan data, etika, praktik yang baik, dan penggunaan fasilitas dan peralatan yang tepat.

Kedua, berkaitan dengan pekerjaan. Kurangnya manajemen yang baik saat mempekerjakan orang dapat membahayakan perusahaan. Oleh karena itu, tanggung jawab yang berkaitan dengan keselamatan karyawan harus dijelaskan dengan jelas. Semua pekerja harus mematuhi rencana dan peraturan perusahaan. Selain itu, perusahaan harus mengawasi dan mengelola karyawan mereka, melacak perilaku abnormal mereka, dan menghentikan

mereka jika diperlukan. Para manajer harus memimpin dengan memberi contoh dan mematuhi strategi keamanan perusahaan, peraturan, dan mekanisme pengendalian risiko. Manajer senior (misalnya CFO) bertanggung jawab atas keputusan strategis dan kegiatan yang terkoordinasi, tanggung jawab manajemen mereka adalah memastikan bahwa karyawan mengidentifikasi dan memenuhi tanggung jawab keamanan berikut ini: Memahami peran dan tanggung jawab keamanan informasi mereka sebelum mengizinkan akses ke informasi rahasia atau sistem informasi; Mendapatkan panduan bagi perusahaan untuk menyatakan ekspektasi keamanan mereka; Kesadaran keamanan yang terkait dengan peran dan tanggung jawab keamanan mereka mencapai tingkat tertentu; Mematuhi syarat dan ketentuan penunjukan, termasuk strategi keamanan perusahaan dan metode kerja yang sesuai; Terus memiliki keterampilan dan sumber daya yang sesuai; Semua karyawan bertanggung jawab untuk menjaga keamanan lingkungan kerja mereka Perusahaan harus secara teratur menilai personil yang terlibat dalam pekerjaan yang berhubungan dengan keselamatan. Ada dua jenis penilaian: penilaian kualitas personel dan penilaian bisnis. Penilaian kualitas terutama mengacu pada ideologi dan politik, seperti apakah karyawan mematuhi hukum, peraturan, dan kebijakan yang relevan, disiplin perusahaan, dan etika profesional dan sikap bisnis yang tepat. Penilaian bisnis terutama mengacu pada pengetahuan bisnis dan keterampilan operasional. Perusahaan harus menangani pekerja yang melanggar peraturan keselamatan dan mempertimbangkan jenis, intensitas, dan faktor-faktor yang mempengaruhi perusahaan. Penanganan pelanggaran dapat membantu karyawan menghindari melanggar peraturan keselamatan perusahaan, perubahan pekerjaan, dan pemutusan hubungan kerja. Ada banyak kerusakan yang disebabkan oleh karyawan terhadap perusahaan dalam bisnis e-commerce. Misalnya, karyawan mungkin tidak puas dengan perusahaan karena mereka ditegur, diturunkan pangkat, ditangguhkan, dan ditangguhkan dari akses ke sistem. Mereka kemudian melakukan pembalasan terhadap perusahaan, yang pada akhirnya menyebabkan kerusakan pada paket sistem pemutusan hubungan kerja dan perubahan. Ini harus memastikan bahwa karyawan melakukan tanggung jawab keamanan yang tetap berlaku setelah pemutusan hubungan kerja dan perubahan, termasuk persyaratan keamanan dan tanggung jawab. Perusahaan juga harus mengubah tugas keamanan mereka saat ada perubahan pekerjaan.

Selain itu, karyawan yang dipecat atau pindah harus mengembalikan semua aset berharga, termasuk dokumen, peralatan, kartu akses, perangkat lunak, buku panduan, dan informasi yang tersimpan di media elektronik; memastikan bahwa semua informasi yang relevan ditransfer dari peralatan karyawan sendiri dan dikembalikan ke perusahaan jika informasi tersebut penting bagi perusahaan. Semua karyawan, kontraktor, atau pengguna pihak

ketiga harus mencabut atau menyesuaikan akses mereka ke informasi dan fasilitas pemrosesan informasi, seperti menghapus kunci, ID, depan, dan mengubah nomor akun dan kata sandi. Ini harus dicatat dan diberitahu kepada perusahaan jika penting bagi operasi yang sedang berlangsung. Sesuai dengan perjanjian dengan pihak eksternal, pihak eksternal dapat menangani pemutusan hubungan kerja. Sangat penting untuk memberi tahu karyawan, pelanggan, dan pihak yang bertanggung jawab atas operasi organisasi tentang perubahan dan pengaturan personil dan organisasi.

2. Otorisasi dan manajemen staf

Otorisasi juga dapat menimbulkan risiko personil dalam e-commerce. Bisnis e-dagang mendapat manfaat dari penerapan sistem manajemen otorisasi yang ideal untuk mengurangi risiko operasi dan pengendalian. Manajemen personel tetap, manajemen pengguna, dan manajemen mitra adalah contoh utama dari manajemen otorisasi. Pertama, orang yang akan bekerja di jabatan tersebut harus ditetapkan. Semua jenis manajer aplikasi di perusahaan perdagangan elektronik, termasuk manajer, personel teknis, dan pengguna umum, harus menentukan posisi mereka, menentukan sensitivitas posisi, meninjau tingkat kecocokan dengan posisi, dan melatih mereka. Tentukan sensitivitas posisi: Penentuan sensitivitas posisi yang salah juga dapat menyebabkan risiko, seperti penentuan sensitivitas posisi yang salah dapat menyebabkan penyalahgunaan sistem.

Tinjauan kecocokan antara karyawan dan posisi: Setelah sensitivitas posisi ditentukan, karyawan melihat apakah mereka cocok dengan posisi tersebut.

Pelatihan karyawan: Setelah dipekerjakan, karyawan juga harus dilatih. Kedua, manajemen pengguna: Manajemen akun pengguna mencakup manajemen akun pengguna, audit dan inspeksi manajemen, deteksi aktivitas yang tidak sah, dan manajemen perubahan jabatan yang disebabkan oleh pelanggaran. Identifikasi, otentikasi, dan otorisasi akses adalah tujuan utama manajemen akun pengguna, yang meningkatkan keamanan dengan rutin mengaudit dan memverifikasi keabsahan akun dan otorisasi akses. Selain itu, ketika karyawan dipindahkan, dipromosikan, atau dikeluarkan, mereka harus diubah atau dibatalkan. Pengelolaan akun pengguna dimulai setelah karyawan mendapatkan akun sistem dari administrator sistem. Operator sistem membuat akun untuk karyawan sesuai permohonannya, mengesahkan akses, dan mengirimkan informasi akun, seperti ID pengguna dan metode otentikasi. Akun dibatalkan jika karyawan tidak memerlukannya karena pergantian pekerjaan. Pemantauan dan pemeriksaan manajemen: Pemeriksaan audit dan manajemen biasanya mencakup melihat seberapa banyak otorisasi akun yang dimiliki oleh setiap karyawan; kepatuhan terhadap prinsip-prinsip hak istimewa minimum; apakah semua akun aktif dan

diperbarui; dan apakah karyawan telah menerima pelatihan yang diperlukan. Menyelidiki aktivitas yang tidak sah: Audit dan analisis pelacakan audit dapat membantu menemukan aktivitas yang tidak sah, seperti meminta personel yang curang, memaksa sistem penting dan personel aplikasi untuk libur, dan menemukan masalah selama liburan wajib. Metode ini juga membantu menghindari ketergantungan yang berlebihan pada karyawan individu.

Untuk mengawasi perubahan jabatan yang disebabkan oleh penunjukan sementara dan transfer departemen, terutama untuk menjaga status otoritas pembaruan karyawan. Untuk penunjukan sementara, hak akses harus diubah jika posisi diganti untuk sementara. Misalnya, Anda dapat memberikan akses ke karyawan pengganti sesuai kebutuhan dan menghapusnya jika tidak diperlukan ketika seorang karyawan tidak hadir. Jika seorang karyawan berpindah departemen, mereka harus menghapus otorisasi akses dari jabatan sebelumnya dan kemudian memberikan otorisasi akses baru. Jika tidak, ini dapat menyebabkan "penyebaran otorisasi", yang melanggar prinsip izin minimum.

Manajemen keluar: Penghentian otorisasi biasanya digunakan untuk mengelola akses sistem karyawan. Bisnis harus membuat peraturan untuk memastikan akun sistem dibatalkan secara tepat waktu jika otorisasi penghentian terjadi karena pengunduran diri atau pensiun karyawan secara sukarela. Selain itu, ketika karyawan mengundurkan diri secara sukarela, seperti pemecatan, PHK, atau pemindahan tidak sukarela, tindakan harus diambil untuk menghindari masalah keamanan. Karena karyawan yang memiliki kemampuan untuk mengubah kode atau mengubah sistem dapat menyebabkan masalah yang lebih sulit untuk diselesaikan, atau jika mereka tidak ramah, mereka dapat membatasi area aktivitas dan fungsionalitas mereka. Ketiga, pengawasan mitra

Banyak perusahaan e-commerce mempekerjakan mitra untuk membantu mereka dalam operasi tertentu. Perusahaan e-commerce harus memastikan bahwa mitra mereka tidak secara terang-terangan memiliki akses ke data inti dan sumber daya informasi, dan mereka juga harus membuat perjanjian kerahasiaan yang baik untuk perusahaan agar mitra tidak berani dan tidak dapat mengungkapkan data dan informasi internal perusahaan. Dalam perusahaan e-commerce, departemen terkait harus dengan hati-hati menjalankan tugas manajemen, bertindak sebagai manajer, dan membuat sistem untuk menilai kinerja outsourcing layanan keselamatan. Selain itu, mereka dapat meningkatkan pengawasan dan penilaian mitra dan membuat sistem akuntabilitas kecelakaan dan penyelidikan masalah utama sesuai dengan kebutuhan.

8.3.2 Pendidikan dan Pelatihan Keselamatan

Salah satu metode pengendalian risiko personil yang lebih efektif adalah pelatihan dan pendidikan keselamatan karyawan, yang dapat meningkatkan kesadaran keselamatan karyawan dan mendorong budaya integritas. Langkah-langkah ini dapat meningkatkan perilaku karyawan dan memberi mereka rasa tanggung jawab yang lebih besar terhadap pekerjaan mereka. Langkah-langkah ini juga sangat penting untuk mencegah risiko personel, pendidikan, dan pelati.

1. Sangat mementingkan pelatihan keterampilan dan pengetahuan keselamatan

Perusahaan perdagangan elektronik harus memahami betapa pentingnya pendidikan dan pelatihan keselamatan. Meningkatkan kesadaran keselamatan karyawan dan peningkatan pengetahuan dan keterampilan keselamatan adalah dasar dari penerapan manajemen keselamatan perusahaan. Perusahaan perdagangan elektronik harus memberikan pelatihan setelah pelatihan keselamatan untuk memastikan bahwa karyawan memperoleh pengetahuan dan keterampilan tentang keselamatan, serta kesadaran tentang prosedur dan implikasinya.

2. Merumuskan program pendidikan dan pelatihan keselamatan

Saat membuat program pelatihan dan pendidikan keselamatan, informasi yang perlu dilindungi harus dilindungi, dan langkah-langkah yang perlu diambil untuk melindunginya harus sesuai dengan strategi keamanan dan peraturan yang relevan untuk perusahaan perdagangan elektronik. Program pelatihan dan pendidikan keselamatan harus disesuaikan dengan peran, tanggung jawab, dan kemampuan setiap pekerja. Saat merancang program pendidikan dan pelatihan keselamatan, perusahaan tidak hanya harus mempertimbangkan persyaratan keselamatan, tetapi juga harus mempertimbangkan "apa yang harus dilakukan" dan "bagaimana melakukannya", sehingga karyawan memahami tujuan pendidikan dan pelatihan keselamatan dan bagaimana perilaku mereka dapat berdampak pada perusahaan, baik positif maupun negatif.

3. Menentukan konten pelatihan

Ikuti pelatihan tentang undang-undang, peraturan, dan peraturan keselamatan, kesadaran akan keselamatan, pendidikan etika profesional, pelatihan terkait jabatan dan bisnis, pelatihan manajemen keadaan darurat, dll. Untuk memastikan bahwa karyawan memahami tujuan manajemen keselamatan, pelatihan ini juga mencakup pelatihan tentang kebijakan, peraturan, standar, dan standar industri yang relevan.

Kedua, pendidikan kesadaran keselamatan dan etika profesional: Beri tahu karyawan dan mitra bisnis tentang tanggung jawab dan metode pengecualian keselamatan untuk meningkatkan kesadaran dan komitmen keselamatan.

Ketiga, pelatihan yang berkaitan dengan bisnis pekerjaan: elemen berikut termasuk dalam pelatihan yang berkaitan dengan bisnis pekerjaan.

Pelatihan teknologi keamanan informasi umum: Pelatihan teknologi keamanan informasi umum untuk karyawan perusahaan mencakup tidak hanya prosedur keamanan informasi dasar (seperti laporan kejadian keamanan informasi) dan kontrol dasar (seperti keamanan kata sandi dan kontrol malware, dll.), tetapi juga keamanan pembawa informasi yang luas, seperti basis data komputer, kertas dokumen, file manajemen, file privasi pelanggan, surat internal, dan data sensitif lainnya.

Pelatihan teknologi keamanan jaringan: Melaksanakan pelatihan teknis keamanan jaringan untuk personel teknis yang bertanggung jawab atas pengembangan dan pemeliharaan sistem. Isi pelatihan meliputi keamanan jaringan berdasarkan manajemen keamanan, manajemen keamanan dengan komputer dan jaringan; manajemen keamanan platform dan bisnis, manajemen keamanan yang terkait dengan industri dan bisnis utama; area spesifik, seperti manajemen keamanan anti-penipuan; manajemen risiko TI dan audit TI; manajemen kelangsungan bisnis, dll Pelatihan lainnya: Selain pelatihan keamanan di atas, perusahaan e-commerce juga harus melakukan pelatihan sesuai dengan kebutuhan spesifik bisnis mereka. Misalnya, operator platform e-commerce memberikan pelatihan yang diperlukan untuk operator platform dan distributor logistik; mereka memberikan pelatihan yang diperlukan bagi konsumen untuk menguasai norma-norma keamanan transaksi online dan mengurangi risiko transaksi online. Keempat, pelatihan manajemen darurat: Perusahaan e-commerce dapat mengundang pakar industri dengan pengalaman praktis yang kaya untuk melaksanakan pengetahuan manajemen darurat e-commerce dan pelatihan keterampilan profesional bagi karyawan melalui pelatihan terpusat dan demonstrasi di tempat, untuk meningkatkan tingkat pengetahuan mereka tentang manajemen darurat.

4. Melaksanakan program pelatihan

Perusahaan perdagangan elektronik harus mengikuti rencana yang diusulkan untuk memberikan pendidikan dan pelatihan keselamatan. Saat menerapkan program pelatihan, elemen-elemen berikut ini terutama dipertimbangkan.

Pertama, institusi pelatihan. Perusahaan e-commerce dapat menggunakan lembaga pelatihan mereka sendiri untuk melatih karyawan mereka, atau mereka dapat mempercayakan lembaga pelatihan eksternal yang profesional untuk memberikan pelatihan langsung kepada karyawan mereka.

Kedua, memilih jenis pelatihan. Pilihan metode pelatihan terkait dengan kebutuhan bisnis yang realistis. Bisnis dapat menggunakan berbagai pendekatan pelatihan. seperti

pelatihan berbasis jaringan, pelatihan berbasis kerja, pelatihan tatap muka, dll. Pelatihan berbasis web mengacu pada pelatihan yang diberikan melalui internet, biasanya dalam bentuk video atau teks. Pelatihan berbasis kerja mengacu pada pelatihan tentang pekerjaan karyawan, yang dikombinasikan dengan pekerjaan karyawan yang sebenarnya; kekurangannya adalah bahwa itu dapat berdampak pada pekerjaan normal karyawan. Pelatihan diberikan dalam dua cara. Metode pertama adalah pelatihan berbasis latar belakang pekerjaan, yang mencakup tenaga teknis, staf umum, dan manajemen. Metode kedua adalah pelatihan berbasis keterampilan, yang mencakup pelatihan dasar, menengah, dan lanjutan. Kurikulum tradisional sebagian besar didasarkan pada tingkat keterampilan. Di sini, pelatihan ini terutama berfokus pada latar belakang bisnis.

Pelatihan karyawan umum: Perusahaan mendorong karyawan untuk mengajukan pertanyaan dan memberikan panduan khusus untuk masalah tersebut. Pertanyaan yang diajukan oleh karyawan dapat berupa pertanyaan tentang praktik keamanan yang baik, pengelolaan kata sandi, kontrol akses khusus, dan laporan terkait. Karyawan menentukan waktu pelatihan, dan perusahaan harus membuat kebijakan yang sesuai untuk pelatihan personel manajemen. Para manajer juga membutuhkan pelatihan pribadi, seperti diskusi kecil dan lebih banyak pertemuan, seperti staf umum.

Pelatihan untuk karyawan teknis. Pelatihan dapat diberikan kepada tenaga teknis sesuai dengan fungsi kerja dan produk teknis yang terkait.

Keempat, pelaksanaan instruksi. Sangat penting untuk mendorong karyawan untuk berpartisipasi dalam pelatihan agar pelatihan dapat berlangsung dengan baik. Karyawan harus sadar akan manfaat pelatihan dan keselamatan dan relevansinya dengan pekerjaan mereka. Perusahaan perdagangan elektronik harus berusaha mendapatkan pelatihan untuk menyesuaikan diri dengan kemajuan teknologi informasi dan standar keselamatan yang berubah. Konten pelatihan mungkin sudah ketinggalan zaman jika perusahaan menggunakan sistem informasi atau aplikasi baru, atau jika hukum, peraturan, kebijakan, dan aturan berubah. Pada titik ini, perusahaan dapat mengabaikan program pelatihan keselamatan kelima—uji efek pelatihan—jika tidak memberikan informasi terbaru tentang hal ini kepada karyawannya dengan cepat. Perusahaan e-commerce dapat menggunakan berbagai metode untuk mengevaluasi dampak pelatihan. Misalnya, meningkatkan penilaian pengetahuan keselamatan karyawan untuk mendorong karyawan untuk mempelajari keterampilan keselamatan dan latihan darurat yang diperlukan. Pada saat yang sama, organisasi harus memastikan bahwa karyawan memenuhi persyaratan persaingan dan melakukan pemeriksaan berulang. Selain itu, Anda dapat mengevaluasi hasil pelatihan dengan menilai karyawan yang dilatih dan

mengumpulkan umpan balik tentangnya; melihat apakah karyawan mengikuti prosedur keselamatan di tempat kerja setelah dilatih; mengevaluasi pengetahuan yang diajarkan selama pelatihan; dan memantau jumlah dan jenisnya.

8.3.3 Meningkatkan Kesadaran Keselamatan

Untuk perusahaan e-commerce, kesadaran keselamatan karyawan harus ditingkatkan.

1. Ruang lingkup kesadaran keselamatan

Kesadaran keselamatan mencakup semua jenis staf yang bekerja untuk perusahaan e-commerce. Pertama, kesadaran keselamatan para manajer. Keselamatan adalah seluruh proses mendorong orang-orang dan kelompok untuk bekerja sama untuk mencapai tujuan organisasi, dan orang yang berkomitmen untuk mencapai proses ini adalah manajer. Pemahaman, sikap, dan perilaku manajer perusahaan tentang manajemen keselamatan adalah komponen penting dari pekerjaan manajemen keselamatan. Oleh karena itu, peraturan keamanan harus dibuat, rencana pelatihan dan pendidikan keselamatan harus dibuat secara teratur, manajemen senior di semua tingkatan harus dilatih tentang cara memperbaiki teknologi keamanan dan langkah-langkah kerahasiaan, dan organisasi manajemen keamanan harus dibentuk untuk menilai keamanan seluruh sistem dan melaporkan masalah ke manajemen senior. Kedua, kesadaran keamanan administrator sistem. Administrator sistem harus lebih tahu tentang keamanan untuk memastikan bahwa semua akun dan sistem file aman; secara teratur memeriksa keamanan konfigurasi sistem, seperti cadangan disk, saluran, dan peralatan; terus memperbarui versi perangkat lunak utama dan menginstal tambalan sistem terbaru; mengurangi kemungkinan pencurian file kata sandi, menghentikan layanan yang tidak perlu, dan mengurangi jumlah kejadian yang tidak perlu. Ketiga, kesadaran penuh dari pengguna umum. Tingkatkan kesadaran pengguna umum tentang keamanan, pastikan mereka mengikuti pelatihan keselamatan dan mempelajari tentang metode terbaru untuk melindungi diri; jangan berbagi kata sandi dengan orang lain dan sering mengubah kata sandi; jangan mengambil data tinjauan pribadi dari komputer host Anda; dan jangan berbagi data pribadi dengan orang lain. Untuk memastikan bahwa dokumen asli perusahaan, seperti faktur, voucher, keluar, dan pesanan pergudangan, tidak akan bocor; perusahaan secara sadar mematuhi aturan dan peraturan keamanan dan kerahasiaan yang dibuat oleh perusahaan; dan tidak membuat, menyalin, atau menyebarkan informasi yang melanggar hukum atau undang-undang. Keempat, meningkatkan kesadaran untuk menghindari personel luar. Perusahaan menghentikan perilaku yang merugikan karyawannya, membatasi otorisasi karyawannya hingga batas tertentu, berkonsentrasi pada pesaing, dan menghindari spionase bisnis.

2. Meningkatkan kesadaran keselamatan personel

Perusahaan harus melakukan proyek untuk meningkatkan kesadaran keselamatan karyawan sehingga hal pertama yang terlintas di benak karyawan saat mereka bekerja sehari-hari adalah melindungi keselamatan perusahaan. Proyek ini juga harus mengajarkan karyawan untuk lebih peduli dengan keselamatan perusahaan dengan menanamkan rasa tanggung jawab dan tujuan pada mereka yang mengontrol dan memproses data penting.

Pertama, pentingnya proyek peningkatan kesadaran keselamatan personel. Proyek ini dapat membantu karyawan berperilaku lebih baik, yang pada gilirannya meningkatkan keselamatan perusahaan. Ini cukup untuk mengurangi risiko kerusakan yang tidak disengaja atau kerusakan data perusahaan; mengurangi kerusakan atau risiko yang disebabkan oleh pengabaian ancaman keselamatan; dan mengurangi risiko melanggar peraturan perusahaan. Untuk meningkatkan kesadaran keselamatan karyawan, manajer harus melakukan hal-hal berikut: membuatnya sederhana, menarik, dan tidak membebani karyawan; mengulang informasi penting dan memastikan bahwa informasi tersebut mudah diakses dan digunakan; memberi tahu karyawan tentang ancaman keamanan dan cara melindungi informasi penting bagi pekerjaan mereka; dan memimpin dengan memberi contoh.

Ketiga, pengetahuan tentang keamanan proyek Fokus proyek harus pada topik yang berkaitan dengan karyawan: aset berwujud, informasi yang tersimpan, ancaman keamanan jaringan terbuka, hukum pelanggaran privasi, dan teknik penyimpanan, identifikasi, dan pengiriman data dengan aman. Selain itu, proyek yang bertujuan untuk meningkatkan kesadaran personel tentang keselamatan juga menjelaskan kepada siapa Anda harus melaporkan insiden keselamatan.

Keempat, metode untuk meningkatkan kesadaran keselamatan personel dalam proyek. Menggunakan media, jurnal elektronik, film pendek animasi, video berita, pidato, konferensi, aplikasi, brosur, dll., mengadakan ceramah khusus, kasus yang memberi tahu karyawan tentang ancaman yang ada, dan meningkatkan pemahaman keamanan.

3. Peningkatan kemampuan identifikasi risiko personil

Identifikasi risiko adalah langkah pertama dalam manajemen risiko dan pengendaliannya. Meningkatkan kemampuan personel untuk mengidentifikasi risiko dapat secara signifikan mengurangi kemungkinan terjadinya risiko serta kerugian yang disebabkan oleh risiko tersebut. Kemampuan untuk mengidentifikasi risiko personel termasuk pengetahuan bisnis yang kaya, keahlian dalam ilmu pengetahuan dan teknologi, kesadaran keselamatan yang kuat, kemampuan tanggap darurat yang baik, dan kepatuhan yang ketat terhadap prosedur operasi. Dengan menemukan potensi kecelakaan, perusahaan dapat berbagi pengalaman,

meningkatkan kemampuan karyawan untuk menyelidiki dan menangani risiko keselamatandan menanganinya.

8.3.4 Pendidikan Kejujuran dan Pembangunan Budaya Integritas

Pembangunan budaya kejujuran dan pendidikan kejujuran adalah cara penting untuk mengarahkan perusahaan dan anggota masyarakat untuk bersikap jujur dan disiplin, serta meningkatkan kualitas moral mereka.

1. Mempopulerkan pendidikan integritas

organisasi semua kekuatan sosial, mengarahkan subjek pasar untuk bertindak dengan itikad baik sesuai dengan hukum, menciptakan gagasan "mempromosikan bisnis dengan integritas", meningkatkan sistem pengawasan opini publik, memperkuat pengawasan subjek yang melanggar kepercayaan, dan menciptakan tekanan opini publik dan batasan moral terhadap perilaku yang melanggar kepercayaan yang serius.

2. Publisitas integritas yang luas

Faktor internal, seperti fisiologi, tidak hanya mengendalikan dan menggerakkan perilaku manusia, tetapi juga faktor eksternal, seperti lingkungan manusia. Karena itu, perilaku manusia selalu berubah dan berubah, sehingga pengendalian dan pengelolaan perilaku manusia harus dilakukan dengan cara yang dinamis dan berubah-ubah. Oleh karena itu, pembangunan budaya integritas dan pendidikan integritas harus menggabungkan konstruksi reguler dan non-reguler, seperti tinjauan dan insentif.

Digabungkan dengan peristiwa penting seperti Hari Publisitas Kredit Jaringan, Hari Hak Konsumen internasional, Hari Peduli Catatan Kredit Nasional, Bulan Publisitas Bisnis Kredit, Hari Konstitusi Nasional dan Hari Publisitas Hukum Nasional, dan hari libur resmi lainnya, fokus publikasi kebijakan dan peraturan kredit, pengetahuan tentang kredit, dan masalah umum. menjadikan pembawa publisitas integritas lebih baik, meningkatkan frekuensi publisitas integritas, dan meningkatkan kualitasnya.

3. Secara aktif mempromosikan model integritas

membuat topik tentang integritas jaringan, menyebarkan dan mempromosikan berbagai contoh dan perbuatan integritas, dan meningkatkan pendidikan peringatan kasus ketidakjujuran jaringan. Kami akan berkolaborasi dengan departemen terkait dan kelompok sosial untuk mendorong model kredit yang lebih baik untuk orang-orang yang memiliki catatan kredit yang buruk. Kami juga akan mendukung penerapan insentif bersama lintas departemen dan lintas bidang untuk mempertahankan kepercayaan.

Selain itu, menciptakan dan meningkatkan program pelatihan kejuruan manajemen kredit dan sistem evaluasi profesional; meningkatkan pelatihan praktisi kredit; meningkatkan pengetahuan tentang manajemen kredit; menciptakan sistem pendidikan dan manajemen kredit; menandatangani surat komitmen kredit masuk dan melakukan kegiatan pelatihan pengetahuan kredit; dan meningkatkan budaya kredit di perusahaan.

8.3.5 Memperbaiki Mekanisme Pelatihan Personil

Di bidang e-commerce, dibutuhkan orang dari berbagai disiplin yang tahu tentang manajemen, keamanan, dan hukum serta manajemen kredit. Akibatnya, kita harus mementingkan pelatihan dan pencadangan talenta gabungan dan terkait. Ini dapat dicapai dengan beberapa cara.

1. Optimalisasi pendidikan akademik:

Pendidikan akademik dan pendidikan di tempat kerja harus dioptimalkan untuk meningkatkan kuantitas, kualitas, dan pelatihan profesional yang relevan. Ini akan memungkinkan pengembangan bakat yang sangat dibutuhkan dalam industri e-commerce dan bidang terkait. Percepat pelatihan karyawan kredit dan lakukan penelitian tentang teori, manajemen, teknologi, standar, kebijakan, dan elemen lainnya.

2. Promosi, Budaya, dan Budaya Bersama:

Perusahaan dapat bekerja sama dengan perguruan tinggi profesional dan lembaga penelitian ilmiah untuk memfasilitasi pelatihan karyawan. Dengan membuat rencana untuk menarik bakat keamanan, membangun basis data ahli manajemen keamanan e-commerce, dan meningkatkan jumlah dan kualitas pelatihan karyawan yang relevan.

3. Memperkuat pelatihan kejuruan dan sertifikasi kualifikasi

Aktif menggunakan pelatihan kejuruan dan sertifikasi kualifikasi, memperkuat pelatihan manajemen keselamatan perdagangan elektronik, seperti pelatihan personel teknis keamanan yang bersertifikat, pelatihan keamanan informasi untuk pengawas keamanan, dll., dan mendorong pelatihan manajemen kredit.

BAB 9
Sistem untuk meningkatkan Pengawasan dan Optimalisasi Manajemen Keamanan E-Commerce

Seperti proses manajemen lainnya, manajemen keamanan e-commerce membutuhkan pengawasan yang objektif, memadai, dan efektif. Pada yang sama, hanya dengan terus mengoptimalkan manajemen keamanan e-commerce kita dapat menjamin pertumbuhan yang sehat dalam e-commerce.

9.1 Sistem Pengawasan untuk Manajemen Keamanan E-Commerce

Untuk meningkatkan produktivitas, manajemen dan pengawasan keamanan e-commerce adalah bagian manajemen yang relatif terpisah yang dibuat untuk meningkatkan efisiensi. Mengoptimalkan manajemen keamanan e-commerce adalah pilihan yang tak terhindarkan saat menghadapi perubahan lingkungan internal dan eksternal. Namun, dasar pengoptimalan adalah evaluasi dan pemahaman yang tepat dari negara, sehingga sangat penting untuk mengawasi manajemen keamanan e-commerce.

Untuk menjamin bahwa manajemen keamanan e-commerce berjalan dengan baik, mekanisme pengawasan keamanan e-commerce merupakan tugas penting. Hanya pengawasan yang efektif yang dapat menghasilkan manajemen keamanan e-commerce secara keseluruhan yang optimal. Oleh karena itu, tujuan dari manajemen dan pengawasan keamanan e-commerce adalah untuk memastikan bahwa perusahaan e-commerce memiliki kemampuan manajemen keselamatan yang baik, yang mencakup kemampuan inti, kemampuan yang diperlukan, dan kemampuan untuk beroperasi dengan baik. Mekanisme kekuatan dan realisasi manajemen dan pengawasan keamanan e-niaga harus dibuat untuk memastikan bahwa perusahaan e-niaga memiliki ketiga kemampuan tersebut.

9.1.1 Sistem Manajemen dan Pengawasan Keamanan E-commerce yang Dinamis

Keamanan e-commerce mencakup keamanan sistem dan subjek, serta keamanan proses dan tautan untuk seluruh rantai industri e-commerce. Kekuatan manajemen keamanan e-commerce berasal dari semua orang yang relevan dalam seluruh proses e-commerce; peserta manajemen keamanan e-commerce adalah semua orang yang relevan dalam seluruh proses produksi dan distribusi; dan semua penerima manfaat dan peserta yang paling termotivasi untuk secara aktif mendukung dan melaksanakan tanggung jawab pengawasan badan utama.

1. Penyebaran sumber daya yang berkaitan dengan pengawasan dan manajemen keamanan e-commerce

Sumber kekuatan manajemen dan pengawasan keamanan e-commerce adalah badan utama untuk mendorong dan melaksanakan tanggung jawab manajemen dan pengawasan keamanan e-commerce. Kekuatan pendorong pengawasan manajemen keselamatan e-commerce muncul selama proses pengembangan dan pengoperasian e-commerce. Kekuatan pendorong ini dapat memberikan kritik dan saran tentang kesalahan manajemen keselamatan e-commerce atau mendorong peningkatan prosedur manajemen keselamatan e-commerce. Saat ini, ini menjadi sumber utama kekuatan dan visi manajemen keamanan e-commerce, yang mencakup pemerintah dan lembaga afiliasinya, organisasi industri, peneliti manajemen keamanan e-commerce, perusahaan e-commerce, dan konsumen.

Negara dan afiliasinya Di satu sisi, pemerintah akan memberikan banyak bantuan dan dukungan untuk pertumbuhan pesat e-commerce. Untuk mendapatkan keuntungan ekonomi dan sosial dari pertumbuhan e-commerce yang sehat, kita perlu memperkuat manajemen keamanan e-commerce untuk mendorong pertumbuhan yang sehat. Sebaliknya, pemerintah sangat mengkhawatirkan keamanan perdagangan elektronik karena kecepatan transmisi informasi, transaksi yang mudah, rantai industri yang panjang, dan pengaruh sosial yang besar.

Selain itu, ada banyak hubungan yang rumit, banyak jenis dan kategori perilaku transaksi dalam sistem perdagangan elektronik, dan banyak tugas pengawasan pasar yang sangat berat. Oleh karena itu, pemerintah dan lembaga afiliasinya adalah sumber utama manajemen keamanan e-commerce China yang berani dan efektif di China.

Organisasi perusahaan. Kelangsungan hidup dan perkembangan organisasi industri, terutama industri e-commerce, sangat erat kaitannya dengan perkembangan industrinya. Akibatnya, organisasi industri ingin menikmati perkembangan industri yang positif. Dimungkinkan untuk mengatakan bahwa tujuan mereka sejalan dengan tujuan pengembangan industri. Keamanan e-commerce tidak hanya memainkan peran penting dalam pertumbuhan industri tetapi juga merupakan pilar kelangsungan hidup perusahaan industri.

Studi manajemen keamanan e-commerce. Peneliti manajemen keamanan e-commerce sering berbicara tentang berbagai macam masalah tentang manajemen keamanan e-commerce dari sudut pandang teoretis atau profesional. Mereka kemudian membuat rekomendasi atau strategi inovatif untuk membantu orang yang bekerja dalam bidang manajemen keamanan e-commerce menjalankan bisnis mereka dengan benar. Perusahaan konsultan atau lembaga pemikir yang bekerja di bidang manajemen keamanan e-commerce juga dapat dikategorikan sebagai peneliti.

Perusahaan online. Perusahaan e-commerce membutuhkan kesadaran yang kuat tentang cara menjaga keamanan bisnis mereka sendiri. Operator platform perdagangan elektronik terutama berkonsentrasi pada keamanan pemasaran; operator platform terutama berkonsentrasi pada keamanan sistem perdagangan elektronik dan transaksi jaringan. Secara keseluruhan, perusahaan e-commerce mendorong manajemen dan pengawasan keamanan e-commerce melalui penyempurnaan, pendalaman, dan non-globalisasi. Perusahaan e-commerce adalah sumber daya, dan peran mereka dalam sistem manajemen dan pengawasan keamanan e-commerce adalah yang paling penting. Namun, sebagai pelaksana utama dan penanggung jawab, tindakan dan dampak yang dilakukan untuk mendorong manajemen dan pengawasan keselamatan adalah praktis dan efektif.

Klien Konsumen adalah baik konsumen nyata maupun potensial. Mereka menjaga kepentingan mereka sendiri dengan fokus pada kualitas produk, layanan purna jual, dan elemen lain. Selain itu, mereka secara efektif mendorong implementasi manajemen dan pengawasan keamanan e-commerce mereka dalam proses menjaga kepentingan mereka sendiri. Namun, pemahaman konsumen tentang pemeliharaan keamanan e-commerce berbeda dalam manajemen dan pengawasan keamanan e-commerce, dan posisinya sebagai sumber kekuatan manajemen keamanan e-commerce tidak stabil atau memadai.

2. Basis pengembangan pengawasan dan manajemen keamanan e-commerce

Pengawasan dan evaluasi yang efektif adalah inti dari manajemen keamanan e-commerce. Untuk e-commerce, sebuah sistem yang membutuhkan kerja sama masyarakat, memastikan pengawasan merupakan dorongan yang kuat selain implementasi kerja dan inspeksi komparatif. Kekuatan pendorong yang kuat sangat penting untuk mendorong manajemen dan pengawasan keamanan e-commerce. Oleh karena itu, pemahaman yang mendalam tentang prinsip-prinsip dasar pengawasan dan manajemen keamanan e-commerce diperlukan. Komponen berikut membentuk dasar manajemen keamanan e-commerce dan kekuatan pengawasan.

Keadilan sosial dipromosikan dan dipertahankan. Salah satu cara utama untuk mengoperasikan masyarakat informasi kontemporer adalah e-commerce. Pengoperasiannya tidak hanya mencakup penyelesaian, penjualan, atau konsumsi transaksi bisnis, tetapi juga melibatkan masalah keadilan sosial. Masalah keadilan sosial utama dalam e-commerce adalah seberapa dekat dan seberapa responsif terhadap nilai-nilai sosial dasar, seperti etika sosial dan komoditas jaringan dasar, serta sistem nilai yang ada yang dipengaruhi oleh konsumsi jaringan.

Untuk mempertahankan dan mempertahankan kepentingan umum. Sangat sulit untuk menentukan batas-batas kepentingan publik, tetapi itu lebih sulit di dunia maya. Akibatnya,

telah menjadi kebiasaan untuk menggunakan pengabaian kepentingan publik. Dengan demikian, perlindungan kepentingan publik dan usulan telah menjadi dasar kekuatan manajemen dan pengawasan keamanan e-commerce. Dalam e-commerce, kepentingan publik terutama berkaitan dengan melindungi kepentingan pihak ketiga yang tidak melakukan kesalahan dalam kegiatan e-commerce, serta mencegah pelanggaran bersama oleh kedua belah pihak terhadap kelompok atau kepentingan individu yang tidak ditentukan. Selain itu, banyak kepentingan publik baru telah muncul sebagai akibat dari munculnya komunitas jaringan dan masyarakat virtual. Para peneliti, pemerintah, dan afiliasi mereka di bidang manajemen keamanan e-commerce sangat tertarik untuk mendukung dan melindungi kepentingan publik jaringan, terutama yang berkaitan dengan e-commerce.

Perlindungan hak dan kepentingan setiap orang serta pengoptimalan lingkungan hidup Salah satu tujuan utama manajemen keamanan e-commerce adalah perlindungan hak dan kepentingan individu serta optimalisasi lingkungan hidup. Namun, mereka relatif umum dan memiliki sifat yang bersifat individual, mementingkan diri sendiri, seringkali mengabaikan keamanan sistem secara keseluruhan dan mengabaikan peningkatan atau optimalisasi yang tidak berkaitan dengan kepentingan penting mereka sendiri. Selain itu, pemerintah akan memberikan perhatian yang moderat atau mendorongnya untuk melindungi hak dan kepentingan individu serta optimalisasi lingkungan hidup.

Memelihara struktur organisasi perusahaan dengan transaksi jaringan sebagai dasar Dengan pesatnya pertumbuhan e-commerce, metode perdagangan, tautan perdagangan, dan bahkan produk dan layanan baru muncul tanpa henti, tetapi risiko yang menyertainya akan berdampak besar pada tatanan bisnis. Misalnya, dukungan kredit jaringan dan bantuan untuk subjek ekonomi mikro sangat jelas. Namun, sejumlah besar individu yang tidak termasuk dalam pasar secara tidak sadar melakukan intervensi di bawah publisitas yang salah, yang berdampak negatif pada subjek yang relevan. Pemerintah dan afiliasinya adalah lembaga utama yang menjaga tatanan bisnis dengan transaksi jaringan sebagai inti. Organisasi industri juga memainkan peran penting dalam hal ini.

3. Manajemen keamanan dan pengawasan e-commerce

Aspek-aspek berikut menunjukkan peran utama sumber daya manajemen dan pengawasan keamanan e-commerce:

Pertama, mulai melakukan tugas manajemen dan pengawasan penuh e-commerce. Memulai manajemen dan pengawasan keamanan e-commerce adalah inti dari semua tugas dan sumber daya manajemen keamanan e-commerce. Ini memastikan bahwa setiap tautan ke manajemen keamanan e-commerce berada di bawah pengawasan yang kuat dan memberikan

dukungan yang diperlukan untuk menjalankan tugas sistem e-commerce. Saat ini, ada tiga keadaan yang mungkin terjadi saat mengelola keamanan e-commerce. Pertama, pengembangan sebelum spesifikasi. Manajemen keamanan e-commerce mungkin tidak berguna karena dorongan pengembangan dan kesadaran normatif. Terlalu banyak kesalahan atau pemahaman yang menyimpang dari keadaan sebenarnya dapat menyebabkan kerusakan yang sangat parah yang tidak dapat diperbaiki. Yang kedua adalah spesifikasi sebelum pengembangan, yang memudahkan pengawasan dan mencegah inovasi saat perencanaan. Ketiga, inovasi dan peraturan, yang mencakup hasil manajemen keselamatan yang baik dan risiko keselamatan yang rendah.

Yang kedua adalah mengidentifikasi secara objektif, apriori, dan akurat fenomena dan kecenderungan yang bertentangan dengan keamanan e-commerce. Sebagai akibat dari fakta bahwa selalu ada bukti yang harus diikuti selama proses pengembangan e-commerce, menemukan secara objektif, objektif, dan akurat fenomena dan tren yang bertentangan dengan keamanan e-commerce merupakan tugas yang sangat penting. Ini bahkan dapat dianggap sebagai bagian terpenting dari rantai manajemen dan pengawasan keamanan e-commerce.

Ketiga, mengawasi orang-orang yang bertanggung jawab atas manajemen keamanan e-commerce. Sistem hukum, teknologi, standar, dan instruksi dapat digunakan untuk mengawasi topik manajemen keamanan e-commerce. Pengawasan hukum bertujuan untuk memantau dan mengawasi kepatuhan terhadap sistem hukum dari subjek yang bertanggung jawab dan sistem hukum yang relevan, memastikan seluruh proses e-commerce berjalan sesuai dengan peraturan dasar, dan mencegah risiko dan masalah keamanan yang disebabkan oleh pelanggaran sistem. Pengawasan teknis mengacu pada apakah pihak yang bertanggung jawab untuk mengawasi telah mengikuti langkah-langkah teknis terbaik, tindakan teknis yang tepat, dan perbaikan teknis yang sesuai untuk menjamin pengoperasian e-commerce. Pengawasan standar mencakup semua jenis standar teknis dan aturan bisnis; peraturan perundang-undangan dan persyaratan wajib lainnya tidak perlu diperhatikan karena mereka dapat menyebabkan masalah yang serius dalam manajemen keamanan e-commerce. Selain itu, bahaya atau kerugian yang ditimbulkan oleh kemajuan e-commerce tidak boleh diabaikan. Norma teknis dan aturan komersial dapat digunakan untuk memantau bisnis di seluruh rantai industri e-commerce. Pengawasan penyuluhan berarti mengawasi pekerjaan orang-orang yang bertanggung jawab atas manajemen keselamatan e-commerce untuk meningkatkan motivasi mereka, kemampuan mereka, dan kemungkinan mencapai tujuan mereka.

Keempat, membangun dan menjaga titik dukungan transformasi. Lebih sulit untuk mengawasi sistem yang sedang dalam masa transisi daripada sistem yang stabil secara objektif. Faktanya, lebih mudah untuk mengubah bisnis konvensional daripada bisnis e-commerce. Oleh karena itu, membangun dan mempertahankan titik dukungan yang tepat dan efisien sangat penting selama proses transformasi e-commerce. Namun, pada saat yang sama, risiko transformasi akan meningkat secara signifikan jika titik dukungan hilang, dan masalah keamanan sering kali lebih besar daripada keadaan stabil yang tidak berubah.

4. Pengawasan laba bergulir mekanisme transmisi daya keamanan e-commerce

Manajemen dan pengawasan keamanan e-commerce membutuhkan sumber daya yang jauh dari cukup selain mekanisme transmisi daya yang tepat dan efektif. Pengawasan yang efektif adalah dasar manajemen keamanan e-commerce, dan transmisi daya adalah satu-satunya cara untuk mempromosikan dan mempertahankan pengawasan tersebut. sebagai ditunjukkan Untuk memulai transmisi daya manajemen dan pengawasan keamanan e-niaga, tujuan manajemen keamanan e-niaga adalah titik awal. Ini mencakup dua kategori tuntutannya sendiri dan tuntutan kesejahteraan masyarakat. Tuntutannya sendiri mencakup tuntutan nilai sosial dan ekonomi subjek pengawasan, dan tuntutan kesejahteraan masyarakat lebih didasarkan pada pengejaran nilai sosial dan publik. Keadaan keamanan e-commerce yang jelas, bentuk, dan target manajemen keamanan e-commerce disesuaikan dengan hasil evaluasi dan disesuaikan dengan target manajemen keamanan e-commerce dalam putaran mekanisme pengawasan berikutnya disebabkan oleh dorongan bersama dari dua jenis tuntutan ini, pengawasan keamanan e-commerce ke dalam tahap konstruksi dan pengawasan.

9.1.2 Membangun Manajemen dan Pengawasan Keamanan E-commerce

Keamanan seluruh proses e-niaga adalah inti dari manajemen keamanan e-niaga. Manajemen keamanan e-commerce harus menghubungkan dan mencocokkan setiap tautan selama proses e-commerce, tetapi harus diingat bahwa keamanan setiap tautan selama proses e-commerce adalah inti dari keamanan keseluruhan. Oleh karena itu, pengawasan dan manajemen keamanan e-commerce harus menjadi langkah-langkah keseluruhan untuk memantau dan mengawasi setiap tautan. Evaluasi, penemuan, dan pembuangan adalah tiga elemen utama dalam proses mewujudkan manajemen keamanan e-commerce.

1. Salah satu hubungan penting dalam manajemen dan pengawasan keamanan e-commerce adalah evaluasi

Meskipun visi super harus digunakan untuk menjamin situasi manajemen keamanan e-commerce, hal pertama yang harus dilakukan adalah melakukan evaluasi yang akurat, objektif,

dan menyeluruh tentang manajemen keamanan e-commerce. Evaluasi kualitatif dan kuantitatif adalah jenis evaluasi yang saling memverifikasi dan melengkapi satu sama lain. Selain uji kuantitatif, evaluasi kualitatif membutuhkan dukungan bukti kuantitatif dan bukti praktis. Di sisi lain, evaluasi kualitatif harus memberikan garis besar sifat dan jalan kualitatif yang jelas. Saat ini, evaluasi kualitatif dilakukan dengan cepat dan membutuhkan sedikit data dan kondisi pada tahap awal. Namun, evaluasi kualitatif relatif kurang akurat dan hasilnya akan sangat mempengaruhi manajemen keamanan e-commerce. Evaluasi kuantitatif juga berjalan lambat dan bahkan mungkin tidak dilakukan sepenuhnya karena kesulitan mendapatkan data, tetapi hasilnya lebih obyektif dan tidak akan berdampak negatif.

2. Tautan utama dalam manajemen dan pengawasan

keamanan e-commerce adalah penemuan. Penemuan adalah kunci dalam manajemen keamanan e-commerce. Apakah berbagai masalah yang muncul dalam aktivitas e-commerce dapat ditangani dengan cepat menentukan apakah pengawasan berfungsi dengan baik. Ini juga menentukan apakah pendekatan dan tindakan yang tepat dapat diambil untuk mendorong optimalisasi manajemen keamanan e-commerce.

3. Dalam hal manajemen dan pengawasan keamanan e-commerce, pembuangan

Penyatuan akan berdampak buruk jika tidak ada sistem, otoritas, atau aturan yang kuat. Oleh karena itu, masalah harus ditangani dengan efektif oleh pengawasan sesuai dengan kepatuhan. Berdasarkan evaluasi dan penemuan masalah yang tepat waktu, tidak tepat secara kualitatif dan pembuangan sama dengan tidak memiliki visi yang sangat baik.

Langkah-langkah pembuangan yang ketat dan dilembagakan memastikan bahwa mekanisme pencegahan, hukuman, dan pengawasan memiliki peran penuh. Mekanisme pengawasan mirip dengan modul kontrol manajemen keamanan e-niaga, yang digunakan untuk memastikan bahwa manajemen keamanan e-niaga tetap pada jalurnya dan mencapai tujuan. Karena pesatnya perkembangan e-commerce, manajer juga harus mempelajari dan mengeksplorasi mekanisme untuk meningkatkan efektivitas manajemen keamanan e-commerce.

9.2 Strategi untuk Meningkatkan Manajemen Keamanan E-Commerce

Pengaturan sistematis yang bertujuan untuk mendorong pengembangan manajemen keamanan yang berkelanjutan dengan The Times, menyelesaikan krisis, dan bahkan menghilangkan ancaman sebelumnya dikenal sebagai mekanisme optimalisasi manajemen keamanan e-commerce.

9.2.1 Mengoptimalkan Manajemen Keamanan E-Commerce

Pengoptimalan manajemen keamanan e-commerce adalah prosedur pengoptimalan manajemen yang khas. Optimalisasi manajemen berarti menciptakan ide kreatif dalam kondisi spasial dan temporal tertentu dan mengubahnya menjadi produk, layanan, atau metode operasi yang bermanfaat melalui perencanaan, organisasi, koordinasi, kontrol, umpan balik, dan kontrol. Sistem memiliki sumber daya biologis, abiotik, modal, informasi, energi, dan sumber daya lainnya untuk mengoptimalkan konfigurasi dan memenuhi kebutuhan aliran biologis, abiotik, aliran abiotik, dan aliran abiotik.

Teori manajemen, teori sistem, sistem, prosedur kantor, alat, dan inovasi adalah semua bagian dari optimalisasi manajemen. Optimasi manajemen dapat diuraikan menjadi inovasi dari fungsi manajemen seperti tujuan, rencana, implementasi, kontrol, penyesuaian, dan pengambilan keputusan. Ini didasarkan pada fungsinya. Jenis inovasi termasuk inovasi strategis sistem bisnis, inovasi model, inovasi proses, inovasi standar, inovasi konsep, inovasi struktur, dan inovasi sistem. Optimasi manajemen keamanan e-commerce dapat didefinisikan berdasarkan gagasan manajemen tinjauan sebagai berikut:

Optimalisasi manajemen keamanan e-commerce adalah istilah yang mengacu pada manajemen keamanan e-commerce yang dipengaruhi oleh elemen-elemen baru dari manajemen, seperti konsep, sistem, teknologi, dan teknik manajemen. atau komponen proses (seperti aliran informasi, logistik, dll.) Kombinasi sistem operasi manajemen keamanan e-commerce untuk mencapai tujuan proses manajemen keamanan secara lebih efisien.

Dalam manajemen keamanan e-commerce, penting untuk mendorong setiap tautan manajemen keamanan e-commerce untuk dioptimalkan, dan pengoptimalan ini dilakukan secara berkelanjutan dalam loop logis dan loop tertutup, yang merupakan saluran manajemen keamanan e-commerce.

9.2.2 Pentingnya dan Tujuan Mengoptimalkan Manajemen Keamanan E-commerce yang Berkelanjutan

Optimalisasi manajemen keamanan e-commerce adalah proses mengalokasikan semua sumber daya untuk mencapai tujuan tertentu dalam konteks tertentu dan memilih gabungan terbaik. Permintaan keamanan e-commerce adalah faktor utama yang mendorong optimalisasi manajemen keamanan e-commerce.

1. Sangat penting untuk mengoptimalkan manajemen keamanan e-commerce

Meningkatkan efektivitas manajemen keamanan e-commerce adalah tujuan dari kesadaran akan pengoptimalan manajemen keamanan e-commerce. Pengoptimalan sangat penting dalam lingkungan yang statis karena perubahan input dan output. Namun, dengan munculnya The Times, perusahaan e-commerce dan lingkungan sekitarnya telah berubah secara signifikan, mengoptimalkan kekuatan tidak hanya dari perusahaan e-commerce itu sendiri dan lebih banyak dipengaruhi oleh lingkungan sekitarnya, tetapi juga menyoroti pengoptimalan manajemen keamanan perdagangan elektronik dalam e-commerce itu sendiri dan seluruh sistem. Di satu sisi, kemajuan teknologi informasi mendorong pertumbuhan e-commerce yang pesat, yang mengarah pada persyaratan keamanan e-commerce yang lebih tinggi, dan juga mendorong optimalisasi manajemen keamanan e-commerce. Sebaliknya, model bisnis dan bentuk e-commerce baru muncul tanpa henti. Kami dapat memenuhi kebutuhan pengembangan keamanan e-commerce hanya dengan terus mengoptimalkan manajemen keamanan e-commerce.

Dalam perspektif lain, tindakan yang merugikan e-commerce muncul dalam arus yang tak ada habisnya dan menjadi semakin kompleks seiring dengan pesatnya pertumbuhan e-commerce. Persyaratan yang lebih mendesak untuk optimalisasi manajemen keamanan e-commerce telah ditimbulkan oleh tindakan destruktif yang didorong oleh kepentingan.

Selain itu, karena operasi bisnis dan proses perdagangan berlangsung dalam jaringan, ketika terjadi kesalahan dalam aktivitas e-commerce, baik stop loss maupun pemulihan akan menghadapi banyak tantangan. Oleh karena itu, manajemen keamanan e-commerce harus dioptimalkan untuk memastikan pencegahan di muka, kontrol dalam proses, dan pasca-pemulihan. Jika pengoptimalan manajemen keamanan e-commerce tidak dilakukan dengan baik, banyak risiko akan mengarah pada kerusakan yang tidak dapat diperbaiki yang permanen.

2. Tujuan adalah untuk meningkatkan manajemen keamanan e-commerce.

Hasil keamanan asli yang optimal dan keuntungan bagi produktivitas manajemen dan keselamatan menunjukkan tujuan pengoptimalan manajemen keamanan e-commerce. Ada dua jenis tujuan untuk pengoptimalan manajemen keamanan e-commerce: tujuan statis dan tujuan dinamis. Sasaran statis dianggap sebagai sasaran horizontal dalam manajemen keamanan e-commerce karena biasanya ditetapkan untuk periode dan lingkungan yang mapan, seperti tingkat default, tingkat deviasi, dan volume pengembalian. Target pengoptimalan dinamis berkaitan dengan proses pengoptimalan kondisi lingkungan, termasuk tingkat sinkronisasi, jumlah kelambatan, dan jumlah kemajuan. Dalam manajemen keamanan e-commerce, sasaran dinamis dapat dianggap sebagai sasaran jangka panjang. Secara umum, indikator dinamis dan

target statis sesuai untuk tujuan jangka menengah dan pendek, sedangkan yang pertama lebih baik untuk tujuan jangka panjang dan menengah.

Analisis metode yang digunakan untuk mengoptimalkan manajemen keamanan e-commerce yang berkelanjutan

Pertama, pertumbuhan e-commerce yang pesat dan optimalisasi manajemen keamanan e-commerce saling berkorelasi. Di era ekonomi digital, ada dua cara berbeda untuk melihat perkembangan pesat e-commerce. Yang pertama adalah pengembangan jaringan bisnis tradisional. Yang lain adalah penciptaan model dan bentuk bisnis jaringan baru. Baik jaringan bisnis konvensional maupun model dan bentuk jaringan bisnis baru, fokusnya adalah mengoptimalkan manajemen keamanan e-commerce menggunakan strategi manajemen dan teknologi manajemen.

Kedua, karena ukuran dan kompleksitas sistem e-commerce terus meningkat, optimalisasi manajemen harus mengimbanginya. Jumlah dan kompleksitas e-commerce terus meningkat di era ekonomi digital. Oleh karena itu, manajemen keamanan e-commerce membutuhkan inovasi pengetahuan lintas bidang yang digerakkan oleh penelitian ilmiah, berorientasi pada aplikasi dengan standarisasi sebagai pusat inovasi teknis, dan informasi sebagai pembawa teknologi informasi sebagai inovasi manajemen yang dipimpin oleh tiga jalur. Seperti yang ditunjukkan oleh Gbr, ketiga jalur ini saling menembus, mendukung, dan memperkuat satu sama lain, serta mendorong inovasi sistem dan manajemen. 9.2.

Ketiga, pengembangan teknologi "cloud" membantu mengoptimalkan manajemen keamanan e- Commerce. Inovasi "awan" adalah ciri dari era ekonomi digital, dan mengandalkan komputasi awan adalah inti dari "awan". Munculnya komputasi awan membuat titik-titik risiko tersebar, yang membuat manajemen keamanan e-niaga menghadapi lebih banyak risiko dan tantangan. Pada saat yang sama, optimalisasi manajemen keamanan e-niaga akan mendapatkan lebih banyak kekuatan dan dukungan.

9.2.3 Implementasi Manajemen Keamanan E-Commerce

Seperti optimalisasi manajemen lainnya, optimalisasi manajemen keamanan e-commerce memerlukan perencanaan dan implementasi yang sempurna. Selain itu, kita harus memahami semua rintangan dan hambatan yang mungkin terjadi, dan membuat semua komponen bekerja sama untuk mendorong manajemen keamanan e-commerce yang optimal.

1. Materi utama yang berkaitan dengan pengoptimalan manajemen keamanan e-commerce

Dalam pengoptimalan manajemen keamanan e-commerce, konsep personel, struktur organisasi, permintaan produk, pemanfaatan sumber daya, dan mekanisme kerja adalah topik

utama. Kelima komponen ini, bersama dengan lima komponen lainnya, membentuk mode pengoptimalan manajemen yang efisien.

Meskipun industri sangat memperhatikan keamanan e-commerce, masyarakat telah memperhatikan konsep personel. Identifikasi masalah keamanan menunjukkan masalah konsep personel dalam manajemen keamanan e-commerce. Bisnis e-commerce terdiri dari banyak subjek yang saling berhubungan. Oleh karena itu, masalah utama pertama dalam optimalisasi manajemen keamanan e-commerce adalah bahwa setiap peserta harus memiliki pemahaman yang sistematis tentang keamanan.

Sistem organisasi Ini adalah bagian yang paling sulit dari manajemen keamanan e-commerce untuk dicapai karena, berdasarkan konsep keamanan sistematis, keamanan perdagangan elektronik memiliki ciri-ciri barang publik semu. Ada banyak masalah untuk menentukan subjek utama dan komponen optimalisasi manajemennya. Pemerintah, lembaga afiliasi terkait, organisasi sosial, dan perusahaan e-commerce harus mendorong pengoptimalan struktur organisasi manajemen keamanan e-commerce karena sifat barang publik semu dari manajemen keamanan e-commerce.

Permintaan untuk produk. Karena keamanan e-commerce memiliki karakteristik barang publik semu, pengelolaannya pada dasarnya dapat diwujudkan melalui produk dan layanan yang berorientasi pada pasar. Oleh karena itu, permintaan produk manajemen keamanan e-commerce harus sesuai dengan strategi pengoptimalan. Meningkatkan permintaan produk keamanan e-commerce secara cepat dan tepat adalah bagian penting dari pengoptimalan manajemen keamanan e-commerce. Dalam proses ini, kita harus mempertimbangkan baik permintaan saat ini maupun permintaan potensial. Menggunakan sumber daya. Untuk manajemen keamanan e-commerce, pengoptimalan juga memerlukan mobilisasi sumber daya dari seluruh sistem untuk mencapainya, karena keefektifannya harus diperiksa dari keseluruhan sistem. Namun, inti dari pengoptimalan manajemen adalah penggunaan sumber daya yang efisien dan peningkatan rasio input-output manajemen keselamatan.

Sistem yang berfungsi Sampai batas tertentu, pengoptimalan mekanisme kerja merupakan inti dari pengoptimalan manajemen keamanan e-niaga, tetapi juga merupakan dampak utama dari pengoptimalan manajemen keamanan e-niaga. Untuk membuat keputusan respons yang sistematis, efektif, dan tepat terhadap risiko dan faktor krisis, pengoptimalan mekanisme kerja memerlukan respons tepat waktu, respons di tempat, transmisi yang lancar, pencocokan kekuatan, dan tanggung jawab.

Perlu diingat bahwa optimalisasi manajemen keamanan e-commerce adalah proses yang bertahap dan terkait dengan melakukan hal-hal yang tidak mungkin.

2. Proposal untuk meningkatkan implementasi manajemen keamanan e-commerce

Manajemen keamanan e-commerce harus melalui empat tahap sebelum dioptimalkan dan diterapkan. Menemukan kekurangan, membuat konsep, mengeksplorasi dan berinovasi, dan mendapatkan pengakuan. Sebelum diimplementasikan, pengoptimalan manajemen keamanan e-commerce akan melewati empat tahap yang sama seperti pengoptimalan manajemen umum.

3. Prosedur untuk menerapkan pengoptimalan manajemen keamanan e-commerce

Pertama, peningkatan komprehensif dan inovasi terpusat diperlukan untuk mengoptimalkan manajemen keamanan e-commerce. Optimalisasi manajemen keamanan e-mail.

commerce adalah untuk meningkatkan efisiensi keamanan sistem e-commerce, sehingga dasar dari efek pengoptimalan evaluasi adalah pengoptimalan status keamanan sistem e-commerce secara keseluruhan; namun, pengoptimalan status keamanan secara keseluruhan seringkali merupakan terobosan terkonsentrasi di beberapa area, yang menghasilkan peningkatan efisiensi keamanan sistem e-commerce. Kedua, proses optimalisasi manajemen keamanan e-commerce selalu bergerak maju. Karena pekerjaan manajemen dasar yang baik dapat memberikan data, data, dan aturan yang tepat, optimalisasi manajemen keamanan e-commerce seringkali terjadi bersamaan dengan pekerjaan manajemen dasar yang baik. Pada saat yang sama, tren spiral yang cukup jelas muncul dari optimalisasi manajemen keamanan e-commerce. Dengan mengoptimalkan manajemen e-commerce dan masalah keamanan, mengambil posisi terdepan, mengoptimalkan secara ilmiah, mengatasi masalah dan tantangan, dan mendorong pengembangan e-commerce yang berkelanjutan,

Sangat mungkin bagi mata pelajaran yang berkaitan dengan perdagangan elektronik untuk mengembangkan kesadaran inovasi dan memberikan peran penuh pada kemampuan mereka untuk optimalisasi dan inovasi. Ini dapat dicapai hanya dengan membentuk tren spiral ke atas dan menciptakan lingkungan yang baik untuk manajemen dan pengoptimalan keamanan perdagangan elektronik. Sangat penting untuk menunjukkan bahwa topik yang berkaitan dengan optimalisasi manajemen keamanan e-commerce adalah bagaimana mengintegrasikan sumber daya dengan lebih efisien untuk mencapai tujuan dan tugas mereka sendiri. Untuk memastikan bahwa optimalisasi manajemen keamanan e-commerce tidak akan terpisah dari kenyataan dan masalah keamanan, optimalisasi manajemen keamanan e-commerce harus menjelaskan penyebab masalah keamanan e-commerce dan faktor-faktor yang mempengaruhinya.

DAFTAR PUSTAKA

Amanah, D., Ramadhanti, N. N., & Harahap, D. A. (2023). *Strategi Pemasaran Online Usaha Minuman Es Campur dan Sop Buah Bhayangkara Sukabumi. BUDIMAS: JURNAL PENGABDIAN MASYARAKAT, 5*(2).

Asir, M., Yuniawati, R. A., Mere, K., Sukardi, K., & Anwar, M. A. (2023). Peran manajemen risiko dalam meningkatkan kinerja perusahaan: studi manajemen sumber daya manusia. *Entrepreneurship Bisnis Manajemen Akuntansi (E-BISMA)*, 32-42.

Fahmi, I., Fachruddin, R., & Silvia, V. (2019, October). Analisis E-Business pada Keputusan Kewirausahaan Bisnis Digital (Sebuah Kajian Literatur Studi). In *prosiding seminar nasional kewirausahaan* (Vol. 1, No. 1, pp. 71-75).

Handoyo, S. (2024). *Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. Heliyon, 10*(8).

Hayati, K. R., Nugraha, I., Sholeha, F., Adriyanto, A., & Astutik, R. L. (2023, November). Penerapan E-Business dan Teknologi Informasi dalam Revolusi Industri 5.0. In *Prosiding Seminar Nasional Waluyo Jatmiko* (pp. 401-410).

Himawan, H. S., Avilla, P. N., Amanda, R., & Zaira, S. (2025). Mengelola Tantangan dan Peluang dalam Bisnis Reseller Online: Strategi Pemasaran, Manajemen Risiko, dan Pengelolaan Keuangan. *Jurnal Visi Manajemen*, *11*(1), 186-202.

Hutahaean, H. D., Mendoza, M. D., & Ambarita, C. F. (2022). SALES LEVEL FORECASTING OF JASMINE FLOWERS WITH EXPONENTIAL SMOOTHING METHOD. INFOKUM, 10(4), 139-145. Retrieved from https://seaninstitute.org/infor/index.php/infokum/article/view/780

Hutahaean, H. D., Rahman, S. M. A., & Mendoza, M. D. (2022, February). Development of interactive learning media in computer network using augmented reality technology. In *Journal of Physics: Conference Series* (Vol. 2193, No. 1, p. 012072). IOP Publishing.

Information Resources Management Association. (2016). *E-commerce: Concepts, methodologies, tools, and applications.* IGI Global.

Li, L., Lin, J., Benitez, J., Luo, X. R., & Mikalef, P. (2025). Seeking decision-making performance: Examining the role of E-commerce capability, digital business intensity, and organizational agility. *Information & Management*, *62*(1), 104064.

Lilisnawati, T., Sen, S., Nuridah, S., Pramanik, D., Warella, S., & Bahtiar, Y. (2023). *Manajemen risiko dalam bisnis e-commerce: Mengidentifikasi, mengukur, dan mengelola risiko*. Jurnal Pendidikan Tambusai.

Mendoza, M. D., Hutajulu, O. Y., & Lubis, A. R. (2022, December). *Interactive E-Business Learning Media Based on Artificial Intelligence.* In *Proceedings of the 4th International Conference on Innovation in Education, Science and Culture, ICIESC* (Vol. 11, p. 400).

Niranjanamurthy, M., & Chahar, D. (2013). *The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2*(7), 2885-2895.

Oktaga, A. T., & Setyowati, W. (2024). *Menavigasi Risiko Pembelian Online: Persepsi Konsumen Dalam Lanskap E-Commerce. Magisma: Jurnal Ilmiah Ekonomi dan Bisnis, 12*(1), 27-47.

Otoritas Jasa Keuangan. (n.d.). *Bijak ber-E-Banking.*

Parete, G. (2015). *Risk management in electronic banking: Concepts and best practices.* Springer.

Paryadi, D. (2018). *Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen. Jurnal Hukum & Pembangunan, 48*(3), 651-669.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty.* Demos.

Rahayu, P., & Rangkuti, S. (2022). *Analisis Manajemen Risiko Penggunaan Aplikasi E-Commerce dalam Transaksi Penjualan CV. Roti Aroma Bakery dan Cake Shop Medan. Bisnis-Net Jurnal Ekonomi dan Bisnis, 5*(1), 55-68.

Rahmadani, R., Mendoza, M. D., Sari, R. D., & Putri, T. T. A. (2019, November). *Implementation of User Centered Design Method in E-Commerce Book Sales Application.* In *ACEIVE 2019: Proceedings of the 3rd Annual Conference of Engineering and Implementation on Vocational Education, ACEIVE 2019*, 16 November 2019, Universitas Negeri Medan, North Sumatra, Indonesia (p. 135). European Alliance for Innovation.

Reynolds, J. (2014). *E-business: A management perspective.* Oxford University Press.

Sari, D. P., & Rahmawati, F. (2020). *Evaluasi Pengendalian Risiko Keamanan Informasi pada E-Commerce Indonesia. Jurnal Manajemen Teknologi, 16*(1), 90–104.

Sukwika, T. (2022). *Manajemen risiko bisnis era digital: Teori dan pendekatan sistem informasi.* Universitas Sahid Jakarta.

Universitas Islam Kalimantan Muhammad Arsyad Al-Banjary. (n.d.). *Manajemen risiko.* Universitas Islam Kalimantan Muhammad Arsyad Al-Banjary.

Universitas Negeri Gorontalo. (n.d.). *Manajemen risiko bisnis era digital (Teori dan pendekatan sistem informasi).* Universitas Negeri Gorontalo.

Van Gestel, T. (2009). *Credit risk management: Basic concepts.* Oxford University Press.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.

Wibowo, A., & Nugroho, Y. (2021). *Analisis Risiko Keamanan Informasi dalam Transaksi E-Commerce. Jurnal Sistem Informasi, 13*(1), 75–88.

Windayani, N. R., Maspiyah, T. W., Alit, R., & Anjani, N. I. (2023, May). Android Learning System Development for Students Family Welfare Department Entrepreneurship Education Course. In *ACEIVE 2022: Proceedings of the 4th Annual Conference of Engineering and Implementation on Vocational Education, ACEIVE 2022, 20 October 2022, Medan, North Sumatra, Indonesia* (p. 71). European Alliance for Innovation.

Zaheer, M. A., Anjum, T., Díaz Tautiva, J. A., & Heidler, P. (2024). Digital transformation of enterprises to enhance sustainability: how does the reputation of digital applications influence the attributes of E-commerce. *Sustainability*, *16*(17), 7365.