KEAMANAN SISTEM INFORMASI

Keamanan sistem informasi adalah subsistem dari organisasi yang mengontrol risiko khusus yang terkait dengan sistem informasi berbasis komputer. Elemen dasar sistem keamanan komputer meliputi: perangkat keras, database, prosedur dan laporan. Misalnya, data pemakaian perangkat lunakdan pelanggaran keamanandapat dikumpulkan dalam waktu nyata, disimpan dalam database, dan digunakan untuk membuat laporan.

Siklus Hidup Sistem Keamanan Informasi

Sistem keamanan elektronik adalah sistem informasi yang perkembangannya membutuhkan aplikasi dari pendekatan siklus hidup. Sistem keamanan komputer dikembangkan dengan menerapkan metode analisis berikut:

1. Analisis sistem.

2. Rancangan sistem.

3. Iplementasi sistem.

4. Operasional, evaluasi, dan kontrol sistem.

Tujuan Masing-masing Fase Siklus Hidup

Fase Siklus Hidup Tujuan

1. Analisis sistem. Menganalisis kerapuhan sistem dari ancaman dan penyingkapan kerugian

2. Rancangan sistem. Merancang keamanan dan rencana untuk pengendalian penyingkapan kerugian yang dikenali.

3. Iplementasi sistem. Mengimplementasikan keamanan seperti dalam rancangan.

4. Operasional, evaluasi dan kontrol sistem. Mengoperasikan sistem, menaksir efektivitas, dan efisiensinya.

Tujuan baru fase pertama dari siklus hidup sistem keamanan adalah menghasilkan laporan analisis kerapuhan dan ancaman. Tujuan fase kedua adalah merancang sekumpulan merancang sekumpulan ukuran pengendalian-risiko yang komprehensif, termasuk ukuran keamanan untuk mencegah kerugian dan rencana kemungkinan mengatasi kerugian yang terjadi. Secara kolektif, keempat fase tersebut merupakan manajemen risiko sistem informasi. Manajemen risiko sistem informasi adalah proses menaksir dan mengendalikan risiko sistem komputer.

. Fase Siklus Hidup dan Laporan ke Dewan Direksi

Fase Siklus Hidup Laporan ke Dewan Direksi

1. Analisis sistem. Ringkasan penyingkapan kerugian.

2. Rancangan sistem. Rencana rinci untuk mengendalikan dan mengatur kerugian, termasuk anggaran sistem keamanan komputer.

3. Iplementasi system operasional, evaluasi dan kontrol sistem. -Penampilan sistem keamanan komputer, termasuk perincian kerugian dan pelanggaran keamanan.

Analisis pemenuhan dan biaya mengoperasionalkan system keamanan.

Sistem keamanan informasi dalam organisasi. Sistem keamanan informasi menjadi efektif, bila diatur oleh kepala petugas keamanan atau chief security officer (CSO). Chief security officer harus melapor langsung kepada dewan direktur untuk memelihara independensi. Kewajiban utama chief security officer adalah memberi laporan kepada dewan direktur, mencakup setiap fase dari siklus hidup.

Menganalisa Kerapuhan dan Ancaman

Dua pendekatan untuk menganalisa kerapuhan dan ancaman sistem, yaitu:

1. Pendekatan kuantitatif.

2. Pendekatan kualitatif.

Pendekatan kuantitatif. Setiap penyingkapan kerugian dihitung sebagai produk dari biaya kerugian dikali kemungkinan terjadinya. Contoh, kemungkinan sebuah kerugian, dilambangkan dengan faktor risiko antara 0 dan 1. Beberapa kesulitan penerapan pendekatan kuantitatif untuk menaksir penyingkapan kerugian, yaitu:

1. Identifikasi biaya per kerugian yang relevan dan kemungkinan yang terkait.

2. Memperkirakan kemungkinan kegagalan pada masa depan, hal ini sulit karena perkembangan teknologi cepat berubah.

Pendekatan kualitatif. Pendekatan kualitatif hanya mendaftarkan kerapuhan dan ancaman sistem, secara subyektif mengatur mereka dengan urutan atas kontribusi mereka kepada penyingkapan kerugian total perusahaan.

Pendekatan kuantitatif dan kualitatif digunakan dalam praktek, dan banyak perusahaan mencampurkan kedua pendekatan tersebut. Terlepas dari pendekatan mana yang digunakan, analisis harus meliputi penyingkapan kerugian dari bidang berikut:

- interupsi bisnis.

- kerugian perangkat lunak.

- kerugian data.

- kerugian perangkat keras.

- kerugian fasilitas.

- kerugian jasa dan karyawan.

Apabila pendekatan kuantitatif yang digunakan, biaya yang dapat diperkirakan adalah sebagai berikut:

- biaya penggantian.

- penyangkalan jasa.

- pertanggungjawaban pihak ketiga.

- interupsi bisnis.

Kerapuhan dan Ancaman

Kerapuhan adalah kelemahan dalam sebuah sistem. Ancaman adalah eksploitasi potensial dari kerapuhan.

Dua kategori ancaman, yaitu: aktif dan pasif. Ancaman aktif meliputi penipuan sistem dan sabotase komputer. Ancaman pasif, meliputi kesalahan sistem, seperti bencana alam, gempa bumi, banjir, kebakaran, dan badai topan. Kesalahan sistem merupakan kegagalan peralatan komponen, seperti kegagalan disk, kekurangan daya.

Ancaman kepada sistem informasi. Sebuah serangan yang berhasil atas sebuah sistem informasi membutuhkan akses perangkat keras, arsip data, atau program kritis. Beberapa penjelasan orang yang terkait dalam sistem informasi adalah sebagai berikut:

1. Karyawan Sistem Komputer

Karyawan sistem komputer, meliputi bagian pemeliharaan, programer, operator, karyawan administratif sistem informasi, dan klerk kontrol data.

2. Bagian Pemeliharaan Komputer Bagian pemeliharaan komputer, memasang perangkat keras dan lunak, memperbaiki kesalahan kecil dalam perangkat lunak.

3. Programer

Programer sistem, menulis program untuk memodifikasi dan memperluas system operasional jaringan. Programer diberi tanggung jawab dengan akses universal kepada semua arsip perusahaan. Programer aplikasi dapat membuat modifikasi yang tidak diinginkan oleh program yang ada atau menulis program baru untuk hal-hal yang tidak diinginkan.

4. Operator Jaringan

Operator jaringan, orang yang meramalkan dan mengawasi operasional jaringan komputer dan komunikasi. Umumnya, operator ditugaskan dengan ijin keamanan tingkat tinggi, untuk secara rahasia mengawasi semua komunikasi jaringan (termasuk pemakai individual yang memasukkan kata kunci).

5. Personil Administrasi Sistem Informasi

Penyelia sistem mendapatkan posisi kepercayaan yang besar. Orang ini memiliki akses rahasia keamanan, arsip, dan program.

6. Klerk Kontrol Data

Klerk kontrol data bertanggung jawab memasukkan secara manual dan otomatis data ke dalam komputer. Ia memiliki kesempatan untuk melakukan kecurangan dengan memanipulasi data masukan.

7. Pemakai

Pemakai terdiri dari kelompok yang heterogen dan dapat dibedakan dari lainnya, karena area fungsional mereka tidak berada dalam pemrosesan data. Banyak pemakai memiliki akses ke data sensitif yang dapat mereka bocorkan kepada para pesaing. Banyak kasus, pemakai bisa mengendalikan masukan komputer yang penting, seperti memo kredit, dan kredit akun.

8. Pengacau

Pengacau adalah orang yang mengakses peralatan, data elektronik, atau arsip tanpa otorisasi yang benar. Pengacau yang menyerang sistem informasi untuk kesenangan dan tantangan disebut hacker. Jenis pengacau lain yaitu: pengacau tidak ketahuan, penyadap kawat, piggybacker, pengacau peniru, dan pencuri dengar.

9. Pengacau yang Tidak Ketahuan

Pelanggan dapat masuk ke dalam area yang tidak terjaga dan membaca data sensitive pada komputer pribadi yang tidak dipelihara. Seorang hacker dapat masuk dan menyerobot atau merusak situs web perusahaan.

10. Penyadap Jaringan

Sebagian besar informasi yang diproses oleh komputer perusahaan bergerak melalui kawat dan kabel. Sebagian informasi dikirimkan dari satu ruang ke ruang lainnya, dan informasi lainnya dapat dikirimkan lintas negara melalui internet. Jalur ini rapuh terhadap penyadap kawat, yang dapat dilakukan dengan alat yang murah misalnya kaset rekamandan sepotong kawat), yang mampu melakukan tugas tanpa memberikan tanda bahwa kawatnya disadap.

11. Piggybacker

Piggybacking merupakan jenis penyadap kawat yang paling canggih. Pelaku memotong informasi yang sah dan mengganti dengan informasi yang lain.

12. Pengacau Peniru

Pengacau peniru adalah orang yang meniru orang lain untuk menipu perusahaan. Pengacau jenis ini menggunakan ID dan kata kunci pemakai yang didapatkan dengan tidak sah untuk mengakses sumber daya elektronik perusahaan.

13. Pencuri Dengar

Tabung sinar katoda atau cathode ray tubes (CRT) standar yang digunakan dalam unit display video umumnya mengeluarkan gangguan elektromagnetik (EMI) pada sebuah frekuensi yang mampu diambil oleh pesawat televisi biasa. Ancaman Aktif kepada Sistem Informasi

Menurut George H. Bodnar dan William S. Hopwood (2001) terdapat enam metode yang dapat digunakan untuk melakukan penipuan sistem informasi adalah sebagai berikut:

1. Manipulasi Masukkan

Manipulasi masukan adalah metode yang digunakan. Orang dapat mengubah masukan tanpa pengetahuan tentang bagaimana sistem komputer beroperasi.

1. Pengubahan Program

Pengubahan program adalah metode yang paling umum digunakan untuk melakukan penipuan komputer. Hal ini dikarenakan membutuhkan ketrampilan pemrograman yang hanya dimiliki oleh sejumlah kecil orang.

1. Pengubahan Arsip Langsung

Banyak kasus, orang-orang akan menemukan berbagai cara memotong proses normal untuk memasukkan data ke dalam program komputer.

1. Pencurian Data

Pencurian data yang penting, misalnya informasi kuantitatif, dan kualitatif tentang kompetitor seseorang. Sejumlah besar informasi dikirimkan antarperusahaan melalui internet. Informasi ini rapuh terhadap pencurian selama dalam perjalanan, hal ini dapat dipotong atau disadap. Disk optis (disket), flash disk, juga dapat dicuri dengan menyelundupkannya ke luar dari perusahaan dalam sebuah kantong atau tas. Barang yang tebal dapat diselundupkan ke luar dalam tempat sampah.

1. Sabotase

Pengrusakan sebuah komputer atau perangkat lunak dapat menyebabkan kebangkrutan sebuah perusahaan. Beberapa kasus, seorang penipu dapat menggunakan sabotase untuk mengecoh dan menutupi penipuannya. Contoh, seorang dapat mengubah database akuntansi, kemudian menutupinya dengan mensabotase disk komputer atau media lainnya. Banyak cara yang menyebabkan komputer mengalami kerusakan serius. Magnet dapat digunakan untuk menghapus pita magnetis dan disk magnetik, dengan meletakkan magnet di dekat media tersebut. Sinar radar dapat memiliki efek serupa bila diarahkan pada sebuah bangunan yang mengandung media magnetik.

1. Penyalahgunaan atau Pencurian Sumber Informasi

Salah satu jenis penyalahgunaan sumber informasi dapat terjadi saat karyawan menggunakan sumber komputer perusahaan untuk bisnis mereka sendiri.

Sistem Keamanan Sistem Informasi

Mengendalikan keamanan dapat dilakukan dengan mengimplementasikan ukuran keamanan dan rencana kemungkinan. Ukuran keamanan berfokus pada pencegahan dan mendeteksi ancaman, rencana kemungkinan berfokus pada memperbaiki efek ancaman. Tidak ada sistem keamanan yang berarti tanpa didukung oleh kejujuran dan kesadaran akan keamanan.

Sistem keamanan komputer harus menjadi bagian dari struktur pengendalian internal keseluruhan perusahaan. Hal ini berarti bahwa elemen dasar dari pengendalian internal (antara lain: pengawasan yang memadai, rotasi pekerjaan, pemeriksaan validitas) adalah penting untuk sistem keamanan komputer. Keamanan sistem komputer merupakan aplikasi khusus dari prinsip pengendalian internal yang telah dibuat untuk masalah tertentu dalam sistem informasi.

Pengendalian untuk Ancaman Aktif

Cara utamamencegah ancaman aktif yang berkaitan dengan penipuan dan sabotase adalah dengan mengimplementasikan urutan lapisan dari pengendalian akses. Filosofi dibalik pendekatan berlapis pada kontrol akses melibatkan sejumlah lapisan kontrol yang memisahkan calon pelaku dari target potensialnya. Tiga lapisan ini yaitu: pengendalian akses tempat, pengendalian akses sistem, dan pengendalian akses arsip. Langkah pertama dalam membangun pengendalian akses adalah menggolongkan semua data dan peralatan sesuai dengan kepentingan dan kerapuhan mereka. Peralatan dan data yang kritis harus diberikan pengendalian yang paling ketat.

Pengendalian akses tempat. Pengendalian akses tempat adalah secara fisik memisahkan orang yang tidak sah dari sumber komputer. Pemisahan fisik, secara khusus diterapkan kepada perangkat keras, area entri data, area keluaran data, perpustakaan data, dan penghubungan komunikasi.

Pengendalian akses sistem. Kontrol akses sistem adalah pengendalian berorientasi perangkat lunak yang dirancang untuk menjaga agar pemakai yang tidak sah tidak menggunakan sistem. Tujuan pengendalian akses sistem adalah untuk mengotentikasi pemakai dengan menggunakan cara seperti ID pemakai, kata kunci, alamat IP, dan alat perangkat keras.

Pengendalian akses arsip. Lapisan terakhir dari pengendalian akses diterapkan pada tingkat arsip. Pengendalian akses arsip mencegah akses tidak sah pada data. Pengendalian akses arsip yang paling fundamental adalah otorisasi dan prosedur untuk mengakses dan mengubah arsip. Semua program penting harus disimpan dalam arsip terkunci, artinya program dapat dijalankan, namun tidak dapat dilihat atau diubah.

Pengendalian untuk Ancaman Pasif

Ancaman pasif meliputi kegagalan daya, dan perangkat keras. Pengendalian untuk ancaman pasif dapat preventif atau korektif. Pengendalian untuk ancaman pasif dapat dilakukan dengan sistem toleran kesalahan dan memperbaiki kesalahan pendukung arsip.

Sistem toleran kesalahan. Sistem toleran kesalahan adalah bila satu bagian dari sistem itu gagal, bagian lainnya segera mengambil alih, dan sistem terus beroperasi tanpa interupsi. Toleransi kesalahan dapat diterapkan pada lima tingkatan, yaitu: komunikasi jaringan, prosesor CPU, DASD, power suply, dan transaksi individual. Jaringan dapat dibuat toleran kesalahan dengan memberikan jalur komunikasi duplikat dan prosesor komunikasi. Dua pendekatan utama untuk prosesor central prosessing unit (CPU) yaitu: sistem protokol berbasis konsensus dan sistem prosesor anjing penjaga (watchdog). Sistem protokol berbasis konsensus berisi jumlah ganjil prosesor, bila satu prosesor tidak sesuai dengan lainnya, maka setelah itu akan diabaikan, sedangkan sistem prosesor watchdog, mengambil alih pemrosesan bila sesuatu terjadi pada prosesor pertama. DASD dibuat toleran kesalahan dengan beberapa metode, termasuk pemeriksaan baca setelah tulis, penguncian sektor buruk, dan pembuatan cermin disk. Keamanan Internet

Internet membuat sebuah jendela elektronik ke dunia luar yang menghilangkan sumber informasi perusahaan secara fisik, sehingga tidak mungkin sepenuhnya mengimplementasikan lapisan pemisahan fisik dari pendekatan akses keamanan yang berlapis. Contoh, perusahaan dapat meletakkan sebuah komputer dibalik pintu terkunci, namun komputer tidak benar-benar terisolasi bila terhubung dengan internet.

Menurut George H. Bodnar dan William S. Hopwood (2001), kerapuhan terhubung internet dapat muncul dari kelemahan dalam lima bidang berikut:

1. Sistem operasional atau konfigurasinya.

2. Server web atau konfigurasinya.

3. Jaringan pribadi dan konfigurasinya.

4. Beragam program server.

5. Prosedur keamanan umum.

Referensi

Bodnar, H.George dan Hopwood, William S., (2001), Accounting Information System,

Prentice-Hall, Inc.