PENGAMANAN SISTEM INFORMASI

Djajasukma Tjahjadi

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

Abstract

Sistem informasi berbasis komputer bukanlah hal yang baru pada masa sekarang ini. Sistem informasi yang handal sangat berkaitan erat dengan sistem pengamanannya. Untuk mengamankan suatu sistem informasi, kita harus terlebih dahulu mengenal ancaman-ancaman yang mungkin timbul. Secara umum ancaman tersebut dapat dikelompokkan atas ancaman pasif dan ancaman aktif. Pengamanan sendiri umumnya dilakukan berdasarkan pengamanan fisik dan pengamanan atas akses.

Key Word : information system, fraud, security

Pendahuluan

Pengembangan suatu sistem informasi umumnya mengikuti tahapan: **analisis sistem**, **perancangan sistem**, **pengembangan dan penerapan sistem**, **pengoperasian, pengawasan** dan **pengendalian sistem**. Pengendalian intern pada tahap-tahap tersebut akan sangat menentukan keandalan informasi yang dihasilkan oleh suatu sistem informasi. Tujuan pengendalian intern untuk masing-masing tahap dapat diuraikan sebagai berikut:

Tahap	Tujuan pengendalian
Analisis sistem	Menganalisis kemungkinan-kemungkinan ancaman yang terjadi, misalnya manipulasi, hacker, sabotase, dll.
Perancangan sistem	Merancang standar dan alat pengamanan sistem dari ancaman, dan rencana pengendaliannya.
Penerapan sistem	Penerapan rencana pengamanan dengan standar dan alat yang telah ditentukan
Pengoperasian, pengendalian sistem	Mengoperasikan sistem untuk menilai efektivitas suatu sistem, dan mengadakan penyesuaian yang diperlukan.

Menelaah Kelemahan Sistem dan Ancaman Terhadap Sistem.

Kelemahan suatu sistem (*vulnerability*) dapat menimbulkan ancaman (*threats*) bagi perusahaan. Ancaman ada yang bersifat aktif, seperti: penipuan melalui

komputer (*computer fraud*), dan sabotase. Ancaman yang bersifat pasif meliputi: kerusakan teknis/ hardware, dan bencana alam (banjir, gempa, kebakaran, dll.)

Kejahatan komputer (*computer crime*) merupakan salah satu bentuk "white-collar crime". Laporan statistik menunjukkan kerugian yang diakibatkan oleh "white-collar crime" jauh lebih besar daripada kriminalitas lainnya seperti: perampokan, pencurian, dll.

Oleh karena itu pengendalian intern pada sistem komputer harus dirancang dengan baik agar tidak memberikan kemudahan bagi karyawan untuk melakukan kejahatan komputer. Ada beberapa fungsi/ jabatan yang karena tugasnya mempunyai akses yang luas ke sistem komputer, antara lain:

1. **Karyawan bagian komputer**, yaitu *computer maintenance persons, programmers, computer operators, computer and information system administrative personnel,* dan *data control clerks*.
2. **Computer maintenance persons**. Meliputi karyawan yang bertugas untuk memasang dan memperbaiki hardware dan software. Umumnya karyawan tersebut mempunyai akses ke operating sistem, sehingga mampu mengubah sistem pengamanan komputer. Akan lebih berbahaya jika seluruh pemasangan hardware dan software dilakukan oleh perusahaan lain.
3. **Programmer**, yang bertugas untuk memperbaiki program maupun mengembangkan aplikasi yang sudah ada. Seringkali seorang programmer mempunyai akses ke seluruh file yang ada. Seorang program dapat mengubah program untuk kepentingan pribadinya atau untuk hal lain yang sifatnya merusak / merugikan perusahaan.
4. **Computer operators**, terdiri dari karyawan yang bertugas untuk mengamati pengoperasian komputer dan komunikasinya. Umumnya seorang computer operator melakukan tugasnya melalui suatu workstation (disebut *system console*) yang aksesnya cukup luas. Timbul kemungkinan karyawan tersebut secara diam-diam mengamati komunikasi data yang sifatnya rahasia melalui workstation ini.
5. **Computer and Information Systems Administrative Personnel**, terdiri dari para supervisor yang mempunyai akses atas program dan data rahasia. Seorang supervisor mempunyai kemampuan untuk menghilangkan password seseorang, sehingga orang tersebut dapat mengakses data yang rahasia.

6. **Data Control Clerks**, yang bertanggungjawab atas seluruh proses pemasukkan data, sehingga mempunyai kemampuan untuk memanipulasi data masukan.

Penyelundup (*intruders*), adalah semua orang yang dapat mengakses peralatan, data komputer secara tidak sah. Penyelundupan bisa dilakukan oleh pihak di luar perusahaan maupun oleh karyawan sendiri yang secara diam-diam mengakses data rahasia. “Hacker” juga termasuk salah satu jenis penyelundup. Jenis penyelundupan lainnya:

1. Penyadap (*wiretrappers*). Seringkali informasi ditransmisikan dari satu bagian ke bagian lain melalui kabel. Penyadapan informasi dapat dilakukan dengan menghubungkan alat khusus pada kabel transmisi tersebut.
2. *Piggybackers*. Dengan cara ini selain informasi yang disadap diganti dengan data yang palsu.
3. *Impersonating intruders*. Penyelundup ini adalah orang lain yang bepura-pura bertindak sebagai salah satu karyawan pada perusahaan tersebut. Umumnya dilakukan dengan memperoleh user ID dan password seseorang karyawan.

Ancaman-Ancaman Terhadap Sistem

Ada 6 ancaman yang dapat dilakukan oleh seseorang untuk mengakses sistem komputer secara tidak sah, meliputi:

1. Input Manipulation. Berdasarkan statistik, cara ini merupakan cara yang paling banyak digunakan karena tidak membutuhkan pengetahuan teknis komputer yang terlalu tinggi. Karena untuk memanipulasi data masukan seseorang tidak perlu mengetahui bagaimana suatu program bekerja.
2. Program Alteration. Cara ini dilakukan dengan pengubahan proses logika program. Dengan demikian si pelaku haruslah memiliki kemampuan pemrograman yang cukup. Si pemrogram umumnya meninggalkan suatu “**trapdoor**”, yaitu bagian dari program komputer yang memberikan celah akses ke file-file penting.
3. Direct File Alteration. Cara ini dilakukan dengan mengubah secara langsung data yang tersimpan pada suatu file tanpa melalui program utamanya.
4. Pencurian data (*data theft*), meliputi juga seluruh bentuk penyadapan.

5. Sabotase, yang dapat dilakukan atas peralatan (hardware) maupun software perusahaan. Sabotase bisa dilakukan oleh saingan perusahaan maupun karyawan perusahaan yang merasa tidak puas, atau untuk menutupi manipulasi. Sabotase yang paling sering dilakukan adalah menghapus data yang tersimpan di harddisk/ disket, dll. Sabotase bisa juga dilakukan seorang programmer dengan menciptakan suatu program untuk melakukan tindakan yang merusak data pada saat yang ditentukan (*logic bomb*). Beberapa bentuk logic bom yang lain adalah: **trojan horse, virus program,** dan **worm**.
6. Penyalahgunaan sumber daya komputer perusahaan untuk kepentingan pribadi.

Pengamanan Sistem Informasi

Pengendalian atas keamanan sistem informasi dilakukan dengan menerapakan cara/prosedur dan alat yang mampu mencegah dan mendeteksi dan terjadinya ancaman-ancaman terhadap sistem. Perusahaan juga perlu membuat rencana penanggulangannya jika ancaman tersebut terjadi. Pengendalian dilakukan dengan menerapkan konsep-konsep pengendalian intern (seperti dibahas pada Bab 5), yaitu sebagai berikut:

Control Environment.

Hal ini merupakan dasar dari efektivitas pengendalian secara keseluruhan. Untuk menciptakan control environment yang mendukung perlu diperhatikan 8 buah faktor, yaitu:

Management Philosophy and Operating Style.

Hal yang paling penting untuk meningkatkan pengamanan suatu sistem informasi adalah menciptakan kesadaran bagi tiap karyawan akan pentingnya hal tersebut. Kesadaran ini sebaiknya dimulai dari manajemen yang posisi lebih tinggi sehingga memberikan contoh bagi para bawahannya.

Struktur Organisasi.

Pembagian tugas dan wewenang pada bagian sistem informasi harus dirancang dengan benar sehingga memisahkan fungsi perancangan sistem, programmer, dan perancangan sistem akuntansi.

Board of Directors and its committee.

Audit committee sebaiknya mendiskusikan hasil yang diperoleh dari para internal auditor dengan para eksternal auditor dan top management untuk mengevaluasi prestasi para penanggungjawab sistem informasi.. Internal Auditor berarti dituntut untuk mempunyai latar belakang sistem pengaman sistem informasi yang baik.

Metode Pendelegasian wewenang dan tanggungjawab dilakukan dengan mendokumentasikan struktur organisasi, kebijakan-kebijakan, uraian tugas dan tanggung jawab (job description).

Metode Pengendalian.

Perusahaan perlu menetapkan anggaran untuk pengadaan peralatan komputer, software, dan biaya operasional. Anggaran ini perlu dibuat secara terperinci untuk menghindari pembelian software dan peralatan yang sebenarnya tidak diperlukan. Pencatatan pemakaian komputer, printer atau alat lain oleh tiap orang/ departemen perlu dicatat untuk mengetahui apakah pemakaian tersebut masih dalam tingkat yang wajar.

Internal Audit Function. Sistem pengamanan harus secara terus-menerus dievaluasi, sehingga dapat diadakan perbaikan-perbaikan yang diperlukan. Setiap perbaikan yang dilakukan haruslah sesuai dengan kebijakan yang telah ditetapkan. Secara periodik harus diadakan pengecekan yang terperinci untuk mendeteksi pengaksesan file yang tidak sah.

Personnel policies and practices.

Pemisahan fungsi, pengawasan, job rotation, forced vacation, dan double check tetap dilakukan pada sistem informasi berbasis komputer. Pemisahan fungsi yang terpenting dilakukan adalah antara bagian pengguna sistem informasi (user) dan bagian perancang sistem informasi, user dan bagian penyimpanan data (librarian). **Job rotation dan forced vacation** juga diterapkan bagi para karyawan yang pekerjaan rutinnya berhubungan dengan file-file penting. Hal ini dapat menghindari atau mendeteksi adanya "**lapping**" secara elektronis oleh bagian yang mengelola kas dan piutang. Pemberhentian karyawan juga perlu mendapat perhatian khusus, agar tidak berakibat buruk bagi perusahaan di kemudian hari. Segera setelah seorang karyawan diberhentikan, maka pada saat itu juga seluruh akses yang ia miliki harus segera ditutup.

Pengendalian atas ancaman-ancaman aktif.

Cara utama untuk melindungi sistem informasi terhadap 6 macam ancaman aktif adalah dengan menerapkan pengendalian *berlapis (layered approach to access control*). Pengendalian berlapis tersebut terdiri dari**:**
site-access controls, system-access control, dan file-access control.

Site-access control.

Tujuan pengendalian ini adalah melindungi peralatan, software, dan data secara fisik. Daerah yang digunakan untuk peralatan, pemasukkan data, pencetakan hasil, penyimpanan data, dan komunikasi data haruslah dipisahkan letaknya secara fisik. Setiap karyawan/ user diharuskan menggunakan kartu identifikasi, penggunaan kunci untuk tiap ruangan (bila perlu dilengkapi pula dengan kunci magnetis, penggunaan password, sidikjari, retina, suara, dll.), petugas keamanan, dan penggunaan kamera. Ruangan pemrosesan data sebaiknya tidak mudah ditemukan.

System-access control.

Pengendalian ini umumnya dilakukan melalui program untuk mencegah penggunaan komputer secara tidak sah. Misalnya dengan penggunaan **user ID** dan **password.**
Beberapa hal penting mengenai password:

1. Password sebaiknya dibuat bertingkat untuk mempersulit akses ke file-file penting. Misalnya password dengan sembilan tingkat, mulai dari tingkat workstation, network, host computer, file server, file catalog, program, database, record, dan data field. Setiap akses haruslah dicatat user ID, tanggal, jam dan file-file yang digunakan.
2. Password haruslah dibuat acak oleh komputer, dan secara periodik tiap user diharuskan untuk mengganti passwordnya. Perlu diberitahukan pula kepada para user agar tidak menggunakan password yang mudah ditebak, misalnya tanggal lahir, nomor telepon, dan hal-hal lainnya yang terkait dengan si karyawan. Password yang baik memanfaatkan kombinasi huruf besar, dan kecil, menggabungkan dua kata yang tidak berhubungan sama sekali.
3. Diberikan batasan jumlah maksimum pemasukkan password yang salah. Jika jumlah ini sudah dicapai, maka user tersebut diblokir sementara sampai penyebab kesalahan password tersebut dapat dijelaskan.

Penerapan password dalam bentuk lain adalah dengan menggunakan konsep "**sign-countersign**". Seorang user memasukkan user ID, kemudian komputer memberikan sandi (*sign*) dan user kembali memasukkan jawaban yang sesuai atas sandi tersebut (*countersign*). Perlu diingat bahwa 1 pasangan kata (sign dan countersign-nya) hanya digunakan satu kali saja.

File-access control.

Lapisan yang terakhir ini diterapkan terhadap seluruh file program dan data perusahaan. Setiap perubahan program haruslah disertai dengan persetujuan tertulis. Hal ini untuk menghindari agar tidak terjadi perubahan program untuk kepentingan pribadi programmer. Programmer harus melalukan pengubahan program pada duplikatnya, bukan pada programmnya yang asli. Dengan demikian perusahaan dapat memeriksa perubahan apa saja yang telah dilakukan oleh programmer. Setiap file harus pula dilengkapi dengan password sehingga tidak sembarang orang dapat melihat atau mengubah isi file tersebut

Data Encryption. **Encryption** adalah proses pengubahan suatu data menjadi sandi (*ciphertext*). Biasanya digunakan untuk menyembunyikan informasi dari penyadapan pada saat transmisi. Proses pengubahan sandi menjadi data aslinya disebut **decryption**, yang memerlukan suatu "kunci" (*key*). Beberapa jenis data encryption adalah:

1. Private-key encryption. Cara ini efektif diterapkan untuk file yang dipakai sendiri, tidak dikirimkan ke orang lain. Proses encryption dan decryption menggunakan satu kunci yang sama. Salah satu contoh adalah DES (Data Encryption Standard) yang dikembangkan oleh IBM, menggunakan kunci sepanjang 56 bit.
2. Public-key encryption. Menggunakan 2 jenis kunci yaitu public key (kunci umum yang diketahui oleh semua orang) digunakan pada tahap encryption, dan satu private key (yang hanya diketahui oleh satu orang) sebagai kunci pada tahap decryption. Salah satu contoh public-key encryption adalah RSA (singkatan dari para penemunya: Rivest, Adi Shamir, and Leonard Adelman), bisa mempunyai kunci sepanjang 1000 bit.

3. Double-key encryption. Menggunakan cara private-key dan public-key. Pada tahap awal, dipilih suatu private-key secara random (khusus untuk suatu pesan). Private-key ini diencryption lagi menggunakan public key, menghasilkan encrypted key. Encrypted key dan encrypted message kemudian dikirim ke suatu tujuan. Artinya si penerima harus dapat menerjemahkan encrypted key dahulu dan kemudian key tersebut digunakan untuk menerjemahkan sandi yang dikirim.

Pengendalian atas ancaman-ancaman pasif

Pengendalian atas musibah seperti bencana alam, kerusakan peralatan, dll, dilakukan dengan rencana yang bersifat preventif dan korektif, terdiri dari

1. **Fault-tolerant systems**. Fault-tolerant system diterapkan baik pada jaringan komunikasi, CPU, DASD, dan sumber listrik, meliputi:
    a. watchdog-processor, yaitu penggunaan processor cadangan. Processor cadangan ini langsung berfungsi begitu processor utamanya rusak.
    b. Read-after-write checks, yaitu pembacaan ulang sector tertentu setelah suatu data disimpan, untuk memastikan apakah proses penyimpanan data tidak mengandung kesalahan.
    c. Bad-sector lockout, yaitu proses pemberian tanda pada sector-sector yang rusak agar tidak dipakai lagi.
    d. Disk mirroring/ disk shadowing, melibatkan proses penyimpanan data yang secara parallel pada dua buah media penyimpanan.

2. **File Backup**. Membuat file cadangan (Backup) merupakan salah satu cara efektif yang dapat dilakukan untuk melindungi data. Ada tiga jenis backup, yaitu
    a. Full Backup, yang membackup seluruh file pada sebuah disk.
    b. Incremental backup, yang membackup file yang diubah sejak backup terakhir.

Referensi

1. Bodnar, George H. and Hoopwood, William S., **Accounting Information Systems**, 4th ed., Allyn and Bacon, 1990.
2. Cushing, Barry E. and Romney, Marshall B., **Accounting Information Systems**, 5th ed.**,** Addison-Wesley Publishing Company Inc., 1990.
3. Page, J. and Hooper, P., **Accounting and Information Systems**, Prentice-Hall, Inc., 1987