MODUL PROTEKSI DAN PERTUKARAN INFORMASI KESEHATAN

PERTEMUAN 6 (ONLINE)

Syefira Salsabila., S.Gz, MKM

PENDAHULUAN

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah “information-based society”. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi).

Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code*) yang digunakan sehingga semakin besar probabilitas terjadinya lubang keamanan (yang disebabkan kesalahan pemrograman, bugs). Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti Internet. Hal ini membuka akses dari seluruh dunia. (Maksud dari akses ini adalah sebagai target dan juga sebagai penyerang.) Potensi sistem informasi yang dapat dijebol dari mana-mana menjadi lebih besar.

Keamanan sistem informasi pada saat ini telah banyak dibangun oleh para kelompok analis dan programmer namun pada akhirnya ditinggalkan oleh para pemakainya. Hal tersebut terjadi karena sistem yang dibangun lebih berorientasi pada pembuatnya sehingga berakibat sistem yang dipakai sulit untuk digunakan atau kurang user friendly bagi pemakai, sistem kurang interaktif dan kurang memberi rasa nyaman bagi pemakai, sistem sulit dipahami interface dari sistem menu dan tata letak kurang memperhatikan kebiasaan perilaku pemakai, sistem dirasa memaksa bagi pemakai dalam mengikuti prosedur yang dibangun sehingga sistem terasa kaku dan kurang dinamis, keamanan dari sistem informasi yang dibangun tidak terjamin.

Hal-hal yang disebutkan diatas dapat disimpulkan bahwa dalam membangun sebuah keamanan sistem informasi harus memiliki orientasi yang berbasis perspektif bagi pemakai bukan menjadi penghalang atau bahkan mempersulit dalam proses transaksi dan eksplorasi dalam pengambilan keputusan. Terdapat banyak cara untuk mengamankan data maupun informasi pada sebuah sistem. Pengamanan data dapat dibagi menjadi dua jenis yaitu : penecegahan dan pengobatan. Pencegahan dilakukan supaya data tidak rusak, hilang dan dicuri, sementara pengobatan dilakukan apabila data sudah terkena virus, sistem terkena worm, dan lubang keamanan sudah diexploitasi.

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat LAN untuk sistem informasinya dan menghubungkan LAN tersebut ke Internet. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan

mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

PROTEKSI

Proteksi adalah mekanisme sistem operasi untuk mengontrol akses terhadap beberapa objek yang diproteksi dalam sistem operasi. Objek-objek tersebut bisa berupa perangkat keras (seperti CPUS, memori, disk, printer, dll) atau perangkat lunak (seperti program, poses, berkas, bass data, dll). Di beberapa sistem, proteksi dilakukan oleh sebuah program yang bernama reference monitor. Setiap kali ada pengaksesan sumber daya PC yang diproteksi, sistem pertama kali akan menanyakan reference

monitor tentang keabsahan akses tersebut. Reference monitor kemudian akan menentukan keputusan apakah akses tersebut diperbolehkan atau ditolak.

Secara sederhana, mekanisme proteksi dapat digambarkan dengan konsep domain. Domain adalah himpunan yang berisi pasangan objek dan hak akses. Masing-masing pasangan domain berisi sebuah objek dan beberapa akses operasi (seperti read, write, execute) yang dapat dilakukan terhadap objek tersebut. Dalam setiap waktu, setiap proses berjalan dalam beberapa domain proteksi. Hal itu berarti terdapat beberapa objek yang data diakses oleh proses tersebut dan operasi-operasi apa yang boleh dilakukan oleh proses terhadap objek tersebut proses juga bisa berpindah dari domain ke domain lain dalam eksekusi.

Implementasi pengamanan sangat penting untuk menjamin sistem tidak diinterupsi dan di ganggu. Proteksi dan pengamanan terhadap perangkat keras dan sistem operasi sama pentingnya.
Pada sistem komputer banyak objek yang perlu diproteksi, yaitu:

1. Objek perangkat keras.
   Objek yang perlu diproteksi antara lain:
   a. Pemroses.
   b. Segment memori.
   c. Terminal.
   d. Disk drive.
   e. Printer.
2. Objek perangkat lunak.
   Objek yang perlu diproteksi antara lain:
   a. Proses
   b. File.
   c. Basis data.
   d. Semaphore.

Proteksi memiliki beberapa tujuan antara lain :

1. Untuk melindungi, memberikan ijin dan mengatur pemakaian sumber daya yang ada dalam sistem tersebut baik sumber daya fisik (memori, diks, prosesor, jaringan komputer) maupun data / informasi.
2. Menjamin sistem tidak di interupsi dan di ganggu
3. Menghindari, mencegah dan mengatasi ancaman terhadap sistem.

DOMAIN PROTEKSI

Yang di maksud domain proteksi yaitu melindungi objek-objek pada sistem komputer agar tidak terjadi kerusakan. Setiap domain harus memiliki nama yang unik dan sekumpulan operasi yang dapat di lakukan terhadap domain. Agar dapat menyediakan mekanisme proteksi berbeda, dikembangkan berdasarkan konsep domain.Domain : himpunan pasangan (objek, hak).Tiap pasangan menspesifikasikan objek dan suatu subset operasi yang dapat dilakukan terhadapnya. Hak dalam konteks ini berarti ijin

melakukan suatu operasi.Proses berjalan pada suatu domain proteksi, yaitu proses merupakan anggota suatu domain atau beberapa domain.

Sistem komputer merupakan gabungan dari banyak proses dan objek. Objek dalam hal ini kita artikan sebagai objek hardware (seperti CPU, segmen memori,printer, disket, dan drive), dan objek software (seperti berkas, program, dan semaphore). Tiap objek mempunyai nama yang khusus yang membedakan mereka dengan lainnya pada suatu sistem, dan tiap-tiap dari mereka dapat diakses hanya melalui operasi yang khusus pula. Secara esensial objek adalah tipe data abstrak.Operasi yang ada memungkinkan untuk bergantung pada objeknya. Contoh CPU hanya bisa dinyalakan. Segmen memori dapat membaca maupun menulis, dimana card reader hanya bisa membaca saja. Drive dapat dibaca, ditulis, ataupun, di-rewound.Berkas data dapat dibuat, dibuka, dibaca, ditulis, ditutup, dihapus; berkas program dapat dibaca, ditulis, dijalankan, dan dihapus.Jelasnya, sebuah proses hanya boleh mengakses resource yang memang dibolehkan. Untuk lebih lanjut, kapan saja, hal ini diharuskan untuk hanya mengakses resource yang memang dibutuhkan saat itu.

HAK AKSES

Hak akses adalah hak yang diberikan kepada user untuk mengakses sistem. Mungkin hak akses adalah hal yang paling mandasar dalam bidang sekuriti. Dalam strategi sekuriti, setiap objek dalam sistem (user, administratir, software, sistem itu sendiri) harus diberikan hak akses yang berguna untuk menunjang fungsi kerja dari objek tersebut. Dengan kata lain, objek hanya memperoleh hak akses minimum.

Dengan demikian, kerja objek terhadap sistem dapat di batasi sehingga objek tidak akan melakukan hal-hal yang membahayakan sekuriti jaringan komputer. Hak akses minimum akan membuat para menyusup dari internet tidak dapat berbuat banyak saat berhasil menembus sebuah *user account* pada sistem jaringan komputer. Hak akses minimum juga bisa mengurangi bahaya yang mengancam sistem dari dalam. Itulah beberapa keuntungan yang dapat di peroleh dari strategi ini.

Subjek (pengguna) dapat memodifikasi atribut akses (read, write, run) setiap objek (sumber daya) yang dibuatnya dengan melakukan proses granting (mengijinkan akses) dan revoking (menolak akses).

Keamanan

Keamanan komputer adalah suatu perlindungan yang diusahakan oleh suatu sistem informasi dalam rangka mencapai sasaran hasil yang bisa diterapkan atau cara untuk memelihara integritas, kerahasiaan dan tersedianya informasi. Tetapi pada saat ini sistem komputer yang terpasang makin mudah diakses. Sistem time sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data menjadi pokok masalah keamanan. Kelemahan ini menjadi amat serius dengan meningkatnya perkembangan

jaringan komputer. Keamanan sistem komputer untuk menjamin sumber daya tidak digunakan atau dimodifikasi oleh orang yang tak berhak. Pengamanan termasuk masalah teknis, manajeral, legalitas dan politis.

Sistem operasi hanya satu porsi kecil dari seluruh perangkat lunak di suatu sistem. Tetapi karena peran sistem operasi mengendalikan pengaksesan ke sumber daya, dimana perangkat lunak lain pengaksesan sumber daya lewat sistem operasi, maka sistem operasi menempati posisi yang penting dalam pengamanan sistem. Pengamanan perangkat lunak cenderung memfokuskan pada pengamanan sistem operasi. Perlu diingat bahwa perangkat lunak aplikasi juga memberi risiko keamanan.

Pengguna sistem komputer sudah tentu memiliki data-data dan informasi yang berharga baginya. Melindungi data-data ini dari pihak-pihak yang tidak berhak merupakan hal penting bagi sistem operasi. Inilah yang disebut keamanan (security)

Keamanan sistem terbagi menjadi 3 yaitu:

1. Keamanan eksternal (external security) : Berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran dan kebanjiran.
2. Keamanan interface pemakai (user interface security): Berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengkases program dan data yang disimpan.
3. Keamanan internal (internal security): Berkaitan dengan keamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data. Istilah keamanan dan proteksi sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah kemanan mengacu ke seluruh masalah kemanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi / melindungi informasi pada sistem komputer.

Masalah-masalah keamanan:

a. Kehilangan data (data loss) dapat disebabkan karena:
    a) Bencana
    b) Kesalahan pernagkat keras dan perangkat lunak
    c) Kesalahan / kelalaian manusia.
    d) Penyusup

Tujuan Security

1. Integritas Data
   Misalnya pengguna yang tidak memiliki autorisasi untuk mengakses data tidak mungkin dapat mengubah atau memodifikasi data.
2. Kerahasiaan Data

Sistem dapat menjamin bahwa data yang telah ditentukan untuk tidak dapat dibaca oleh pengguna lain pada sistem, data tersebut benar-benar aman dan rahasia.

3. Ketersediaan Akses ke Sistem
   Tidak ada seorangpun, sekalipun dengan akses ke sistem dapat menyebabkan sistem menjadi tidak dapat digunakan. Contoh nya dengan serangan denial of service melalui internet.

AUTENTIKASI

Proses pengenalan peralatan, sistem operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer. Autentikasi dimulai pada saat user login ke jaringan dengan cara memasukkan password.

Tahapan Autentikasi:

1. Autentikasi untuk mengetahui lokasi dari peralatan pada suatu simpul jaringan (data link layer dan network layer)
2. Autentikasi untuk mengenal sistem operasi yang terhubung ke jaringan (transport layer)
3. Autentikasi untuk mengetahui fungsi/proses yang sedang terjadi di suatu simpul jaringan (session dan presentation layer)
4. Autentikasi untuk mengenali user dan aplikasi yang digunakan (application layer)

Autentifikasi pemakai

Kebanyakan proteksi di dasarkan asumsi sistem mengetahui identitas pemakai. Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode autentifikasi di dasarkan pada tiga cara, yaitu:

1. Sesuatu yang diketahui pemakai, misalanya :
   a. Password
   b. Kombinasi kunci
   c. Dan sebagainya
2. Sesuatu yang dimiliki pemakai, misalanya;
   a. Badge
   b. Kartu identitas
   c. Kunci
   d. Dan sebagainya
3. Sesuatu mengenai (ciri) pemakai, misalnya;
   a. Sidik jari
   b. Sidik suara
   c. Foto
   d. Tanda tangan

Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "information-based society".

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Jumlah kejahatan komputer (*computer crime), terutama yang* berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain:

a. Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat.

b. Desentralisasi server sehingga lebih banyak sistem yang harus ditangani dan membutuhkan lebih banyak operator dan administrator yang handal. Padahal mencari operator dan administrator yang handal adalah sangat sulit.

c. Transisi dari single vendor ke multi-vendor sehingga lebih banyak yang harus dimengerti dan masalah interoperability antar vendor yang lebih sulit ditangani.

d. Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya.

e. Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.

f. Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code) yang digunakan sehingga* semakin besar probabilitas terjadinya lubang keamanan.

g. Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti Internet. Potensi sistem informasi yang dapat dijebol menjadi lebih besar.

Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (risk management). Lawrie Brown dalam [3] menyarankan menggunakan "*Risk Management Model*" untuk menghadapi ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada Risk, yaitu *Asset*, *Vulnerabilities*, dan *Threats*.

Tabel 1. Kontribusi terhadap Risk

Nama Komponen	Contoh dan keterangan lebih lanjut
Assets (aset)	a. Hardware b. Software

	c. Dokumentasi d. Data e. Komunikasi f. Lingkungan g. Manusia
Threats (ancaman)	a. Pemakai (users) b. Teroris c. Kecelakaan (accidents) d. Crackers e. Penjahat kriminal f. Nasib (act of God) g. Intel luar negeri (foreign intelligence)
	a. Software bugs b. Hardware bugs c. Radiasi (dari layar, transmisi) d. Tapping, crosstalk e. Unauthorized users f. Cetakan, hardcopy atau print out g. Keteledoran (oversight) h. Cracker via telepon i. Storage media

Untuk menanggulangi resiko (*Risk*) tersebut dilakukan apa yang disebut "*countermeasures*" yang dapat berupa:

a. usaha untuk mengurangi *Threat*
b. usaha untuk mengurangi *Vulnerability*
c. usaha untuk mengurangi impak (*impact*)
d. mendeteksi kejadian yang tidak bersahabat (*hostile event*)
e. kembali (*recover*) dari kejadian

PENGENDALIAN KEAMANAN SISTEM INFORMASI

Berkaitan dengan keamanan system informasi, diperlukan tindakan berupa pengendalian terhadap sistem informasi. Kontrol-kontrol untuk pengamanan sistem informasi antara lain:

a) Kontrol Administratif
b) Kontrol Pengembangan dan Pemeliharaan Sistem
c) Kontrol Operasi
d) Proteksi Fisik terhadap Pusat Data

Kontrol-kontrol untuk pengamanan sistem informasi antara lain (Cont):

e) Kontrol Perangkat Keras
f) Kontrol Akses terhadap Sistem computer
g) Kontrol terhadap Akses Informasi
h) Kontrol terhadap Bencana
i) Kontrol Terhadap Perlidungan Terakhir
j) Kontrol Aplikasi

KONTROL ADMINISTRATIF

Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka control dilaksanakan sepenuhnya dalam organisasi berdasarkan prosedur-prosedur yang jelas. Kontrol ini mencakup hal-hal berikut:

a. Mempublikasikan kebijakan control yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi.
b. Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk hal ini adalah proses pengembangan sistem, prosedur untuk *backup*, pemulihan data, dan manajemen pengarsipan data.
c. Perekrutan pegawai secara berhati-hati yang diikuti dengan orientasi pembinaan, dan pelatihan yang diperlukan.
d. Supervisi terhadap para pegawai. Termasuk pula cara melakukan control kalau pegawai melakukan penyimpangan terhadap yang diharapkan.
e. Pemisahan tugas-tugas dalam pekerjaan dengan tujuan agar tak seorangpun yang dapat menguasai suatu proses yang lengkap. Sebagai contoh, seorang pemrogram harus diusahakan tidak mempunyai akses terhadap data produksi (operasional) agar tidak memberikan kesempatan untuk melakukan kecurangan.

KONTROL PENGEMBANGAN DAN PEMELIHARAAN SISTEM

Untuk melindungi kontrol ini, peran auditor sistem informasi sangatlah penting. Auditor sistem informasi harus dilibatkan dari masa pengembangan hingga pemeliharaan system, untuk memastikan bahwa system benar-benar terkendali, termasuk dalam hal otorisasi pemakai system. Aplikasi dilengkapi dengan *audit trail* sehingga kronologi transaksi mudah untuk ditelusuri

Kontrol Operasi

Kontrol operasi dimaksudkan agar system beroperasi sesuai dengan yang diharapkan. Termasuk dalam kontrol ini:

a. Pembatasan akan akses terhadap data
b. Kontrol terhadap personel pengoperasi
c. Kontrol terhadap peralatan
d. Kontrol terhadap penyimpanan arsip
e. Pengendalian terhadap virus

Untuk mengurangi terjangkitnya virus, administrator sistem harus melakukan tiga kontrol berupa preventif, detektif, dan korektif.

Kontrol	Contoh
Preventif	a. Menggunakan salinan perangkat lunak atau berkas yang berisi makro yang benar-benar bersih. b. Mengindari pemakaian perangkat lunak *freeware* atau *shareware* dari sumber yang belum bisa dipercaya. c. Menghindari pengambilan berkas yang mengandung makro dari sembarang tempat. d. Memeriksa program baru atau berkas-berkas baru yang mengandung makro dengan program anti virus sebelum dipakai. e. Menyadarkan pada setiap pemakai untuk waspada terhadap virus.
Detektif	a. Secara rutin menjalankan program antivirus untuk mendeteksi infeksi virus. b. Melakukan pembandingan ukuran-ukuran berkas untuk mendeteksi perubahan ukuran pada berkas c. Melakukan pembandingan tanggal berkas untuk mendeteksi perubahan tanggal berkas.
Korektif	a. Memastikan pem-*backup*-an yang bersih b. Memiliki rencana terdokumentasi tentang pemulihan infeksi virus. c. Menjalankan program antivirus untuk menghilangkan virus dan program yang

	tertular.

Proteksi Fisik terhadap Pusat Data

a. Untuk menjaga hal-hal yang tidak diinginkan terhadap pusat data.
b. Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar.

Kontrol Perangkat Keras

a. Untuk mengatisipasi kegagalan sistem komputer, terkadang organisasi menerapkan sistem komputer yang berbasis *fault-tolerant* (toleran terhadap kegagalan).
b. Pada sistem ini, jika komponen dalam sistem mengalami kegagalan maka komponen cadangan atau kembarannya segera mengambil alih peran komponen yang rusak

Sistem *fault-tolerant* dapat diterapkan pada lima level, yaitu pada:

a. komunikasi jaringan, toleransi kegagalan terhadap jaringan dilakukan dengan menduplikasi jalur komunikasi dan prosesor komunikasi.
b. prosesor, redundasi prosesor dilakukan antaralain dengan teknik *watchdog processor*, yang akan mengambil alih prosesor yang bermasalah.
c. penyimpan eksternal,terhadap kegagalan pada penyimpan eksternal antara lain dilakukan melalui *disk memoring* atau *disk shadowing*, yang menggunakan teknik dengan menulis seluruh data ke dua *disk* secara pararel. Jika salah satu disk mengalami kegagalan, program aplikasi tetap bisa berjalan dengan menggunakan *disk* yang masih baik.
d. catu daya, toleransi kegagalan pada catu daya diatasi melalui UPS.
e. transaksi, toleransi kegagalan pada level transaksi ditanganimelalui mekanisme basis data yang disebut *rollback,* yang akan mengembalikan ke keadaan semula yaitu keadaan seperti sebelum transaksi dimulai sekiranya di pertengahan pemrosesan transaksi terjadi kegagalan.

Kontrol Akses terhadap Sistem Komputer

a. untuk melakukan pembatasan akses terhadap sistem, setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan *password*.
b. sistem-sistem yang lebih maju mengombinasikan dengan teknologi lain. Misalnya, mesin ATM menggunakan kartu magnetic atau bahkan kartu cerdas sebagai langkah awal untuk mengakses sistem dan kemudian baru diikuti dengan pemasukan PIN (*personal identification number*).
c. Teknologi yang lebih canggih menggunakan sifat-sifat biologis manusia yang bersifat unik, seperti sidik jari dan retina mata, sebagai kunci untuk mengakses sistem

d. Pada sistem yang terhubung ke Internet, akses Intranet dari pemakai luar (via Internet) dapat dicegar dengan menggunakan *firewall. Firewall* dapat berupa program ataupun perangkat keras yang memblokir akses dari luar intranet.

Kontrol terhadap Akses Informasi

Ada kemungkinan bahwa seseorang yang tak berhak terhadap suatu informasi berhasil membaca informasi tersebut melalui jaringan (dengan menggunakan teknik *sniffer*). Untuk mengantisipasi keadaan seperti ini, alangkah lebih baik sekiranya informasi tersebut dikodekan dalam bentuk yang hanya bisa dibaca oleh yang berhak.

Studi tentang cara mengubah suatu informasi ke dalam bentuk yang tak dapat dibaca oleh orang lain dikenal dengan istilah **kriptografi**. Adapun sistemnya disebut **sistem kripto**. Secara lebih khusus, proses untuk mengubah teks asli (*cleartext* atau *plaintext*) menjadi teks yang telah dilacak (*cliphertext*) dinamakan **enskripsi,** sedangkan proses kebalikannya, dari *chiphertext* menjadi *cleratext,* disebut **dekrpisi.**

Dua teknik yang popular untuk melakukan enskripsi yaitu DES dan *public-key encryption*.
DES merupakan teknik untuk melakukan enskripsi dan deskripsi yang dikembangkan oleh IBM pada tahun 1970-an. Kunci yang digunakan berupa kunci privat yang bentuknya sama. Panjang kunci yang digunakan sebesar 64 bit. Algoritma yang digunakan mengonversi satu blok berukuran 64 bit (8karakter) menjadi blok data berukuran 64 bit.

Sistem DES yang menggunakan kunci privat memiliki kelemahan yang terletak pada keharusan untuk mendistribusikan kunci ini. Pendistribusian inilah yang menjadi titik rawan untuk diketahui oleh pihak penyadap.

Untuk mengatasi kelemahan sistem kripto simetrik, diperkenalkan teknik yang disebut kriptografi kunci publik. Sistem ini merupakan model sistem kripto asimetrik, yang menggunakan kunci enkripsi dan dekripsi yang berbeda. Caranya adalah dengan menggunakan kunci privat dan kunci publik. Sebagai gambaran, bila pengirim S mengirimkan pesan ke penerima R, ia menggunakan kunci publik R dan kemudian R melakukan dekripsi dengan menggunakan kunci privat R.

Kontrol Terhadap Bencana

Zwass (1998) membagi rencana pemulihan terhadap bencana ke dalam 4 komponen:

a. Rencana darurat (*emergency plan)* menentukan tidakan-tindakan yang harus dilakukan oleh para pegawai manakala bencana terjadi.
b. Rencana cadangan (*backup plan*) menentukan bagaimana pemrosesan informasi akan dilaksanakan selama masa darurat.
c. Rencana pemulihan (*recovery plan*) menentukan bagaimana pemrosesan akan dikembalikan ke keadaan seperti aslinya secara lengkap, termasu mencakup tanggung jawab masing-masing personil.

d. Rencana pengujian (*test plan*) menentukan bagaimana komponen-komponen dalam rencana pemulihan akan diuji atau disimulasikan

Kontrol terhadap perlindungan terakhir

Kontrol terhadap perlindungan terakhir dapat berupa:

a. Rencana pemulihan terhadap bencana.
b. Asuransi.

Asuransi merupakan upaya untuk mengurangi kerugian sekiranya terjadi bencana. Itulah sebabnya, biasanya organisasi mengansurasikan gedung atau asset-aset tertentu dengan tujuan kalau bencana terjadi, klaim asuransi dapat digunakan untuk meringankan beban organisasi

Kontrol Aplikasi

Kontrol aplikasi adalah kontrol yang diwujudkan secara sesifik dalam suatu aplikasi sistem informasi. Wilayah yang dicakup oleh kontrol ini meliputi:

a. Kontrol Masukan
b. Kontrol Pemrosesan
c. Kontrol Keluaran
d. Kontrol Basis Data
e. Kontrol Telekomunikasi

DAFTAR PUSTAKA

https://www.antaranews.com/berita/674301/kasus-serangan-siber-terheboh-2017

https://www.wartaekonomi.co.id/read170777/lima-sektor-bisnis-jadi-sasaran-empuk-serangan-siber-apa-saja.html

Hariningsih.2003.*Sistem Operasi.*Yogyakarta:Graha Ilmu

Riri Fitri Sari dan Yansen Darmaputra.2005.*Sistem Operasi Modern*.Yogyakarta:Andi