Sesi 13 Keamanan Teknologi Informasi

IT Security

Kuliah Online : Dasar Sistem Informasi

Dosen : Ir. Nixon Erzed MT - Tim Dosen Pengantar IT

TUJUAN

Mahasiswa memahami, mengerti dan dapat menjelaskan tentang keamanan teknologi informasi, serangan di internet maupun enkripsi dalam keamanan di internet

Materi

A. Munculnya Kejahatan Komputer
   - 1.1 Penyebab Meningkatnya Kejahatan Komputer
   - 1.2 Aspek-aspek Keamanan Komputer

B. Konsep Keamanan
   - 2.1 Tujuan /Syarat Keamanan
   - 2.2 Lingkup Pengamanan
   - 2.3 Bentuk-bentuk Ancaman
   - 2.4 Program Perusak/Pengganggu
   - 2.5 Prinsip Desain Pengamanan

C. Ancaman Keamanan Komputer
   - 3.1 Serangan Lokal
   - 3.2 Bahaya Internet
   - 3.3 Serangan Hacker

D. Enkripsi
   - 4.1 Konsep Enkripsi
   - 4.2 Cara kerja Enkripsi
   - 4.3 Teknik Enkripsi

E. Keamanan Di Internet
   - 5.1 Titik Pengamanan
   - 5.2 Pengamanan e-mail
   - 5.3 Tanda tangan dan Seftifikat Digital
   - 5.4 Pengamanan Kartu Kredit

F. Pemeliharaan Sistem Komputer
   - 6.1 Menjaga Kinerja System
   - 6.2 Backup Data
   - 6.3 Memelihara Perangkat

A. MUNCULNYA KEJAHATAN KOMPUTER

1.1 Penyebab Meningkatnya Kejahatan Komputer

Maraknya kejahatan computer hingga saat ini ,yang diindikasikan terus mengalamipeningkattan yang disebabkan seperti berikut ini

- Aplikasi bisnis yang mengunakan teknologi informasi dan jaringan computer semakin meningkat .sebagai contoh saat ini mulai bermunculan aplikasibisnis seperti perbankan ,*online banking,Electronic Data Interchange(EDI).*
- Server terdesentralisasi dan terdistribusi menyebabkan lebih banyak system yang harus ditangani. Hal ini membutuhkan lebih banyak operator dan administratorandal yang juga kemungkinan harus disebar keseluruh lokasi. padahal mencari operator dan administrator andal adalah sangat sulit,apalagi harus disebar keberbagai tempat.
- Transisi dari vendor tunggal ke multivendor sehingga lebih banyak system atau perangkat yang harus dimengerti dan masalah interoperability antar vendor yang lebih sulit ditangani.

1.2 Aspek-aspek Keamanan Komputer

Beberapa aspek keamanan computer meliputi hal-halseperti berikut ini:

- Aunthentication, yaitu agar penerima informasi dapat memastikan keaslian pesan tersebut dating dari orang yang dimintai informasi,dengan kata lain informasi tersebut benar-benardari orang yang dikehendaki.
- Integrity,yaitu keaslian pesan yang dikirim melalui sebuah jaringandan dapat dipastikan bahwa informasi yang dikirimkan tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
- Privacy,yaitu lebih kearah data-data yang sifat-sifatnya privat(pribadi)
- Availability, yaitu aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Acces control, aspek ini berhubungan dengan cara pengaturan akses kepada informasi.hal ini biasanya berhubungan dengan masalah autentik dan juga privasi.

B. KONSEP KEAMANAN

2.1 Tujuan /Syarat Keamanan

System computer bias dikatakan sebagai suatu system yang aman jika telah memenuhi beberapa syarat tertentu untuk mencapai suatu tujuan keamanan.Secara garis besar, persyaratan keamanan system computer dapat dibedakan menjadi tiga,yaitu:

a. **Kerahasian** (*secrecy*). secrecy berhubungan dengan hak akses untuk membaca data atau informasi dari suatu system computer.dalam hal ini suatu system computer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang.

b. **Integritas** (*integrity*).integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu system computer.

c. **Ketersediaan (***availability*).availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan .

2.2 Lingkup Pengamanan

Lingkup keamanan adalah sisi-sisi jangkauan keamanan computer yang bias dilakukan.pada prinsipnya pengamanan system computer mencakup empat hal yang sangatmendasar,yaitu:

a. Pengamanan secara fisik

Computer secara fisik adalah wujud computer yang bisa dilihat dan diraba,seperti monitor,CPU,keyboard dan lain-lain.jika computer memang perlu untuk diamankan karena fungsi dan data di dalamnya yang penting,maka pengaman secara fisik dapat dilakukan dengan dengan menempatkan system computer pada tempat atau lokasi yang mudah diawasi dan dikendalikan,pada ruangan tertentu yang dapat dikunci,dan sulit dijankau orang lain,sehingga tidak ada komponen yang hilang.

b. Pengamanan Akses

Ini dilakukan untuk PC yang mengunakan system operasi lagging (penguncian) dan system operasi jaringan.ini dilakukan untuk mengantisipasi kejadian yang sifatnya disengaja ataupun tidak disengaja.

c. Pengaman Data

Pengamanan data dilakukan dengan menetapkan system tingkatan atau hierarki akses dimana seseorang hanya dapat mengakses data tertentu saja yang menjadi haknya

d. Pengamanan Komunikasi jaringan

Jaringan disini berkaitan erat dengan pemanfaatan jaringan republic seperti internet pengamanan jaringan dapat dilakukan dengan mengunakan kriptografi dimana data yang sifatnya sensitive dienkripsi atau disandikan terlebih dahulu sebelum ditransmisikan melalui jaringan tersebut.

2.3 Bentuk-bentuk Ancaman

Bentuk-bentuk ancaman yang munkin terjadi pada system computer baik yang berbasis jaringan maupun tidak pada dasarnya dibedakan menjadi empat kategori,yaitu:

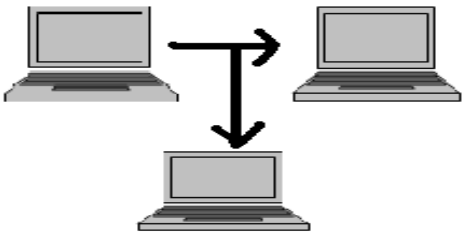
a. Interupsi (Interruption)

Merupakan bentuk ancaman terhadap ketesediaan, dimana suatu data dirusak sehingga tidak dapat digunakan lagi. Tindakan perusakan yang dilakukan dapat berupa perusakan fisik maupun nonfisik. Perusakan fisik umumnya berupa perusakan hardisk dan media penyimpanan lainnya serta pemotongan kabel jaringan. Sedangkan perusakan nonfisik berupa penghapusan suatu file-file tertentu dari system computer

Pengiriman Terjadi Interupsi

b. Intersepsi (interception)

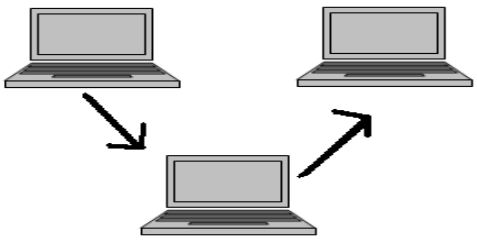
Merupakan suatu bentuk ancaman terhadap secrecy, dimana pihak yang tidak berhak berhasil mendapat hak akses untuk membaca suatu data/informasi dari suatu system computer.



Pengiriman Terjadi Intersepsi

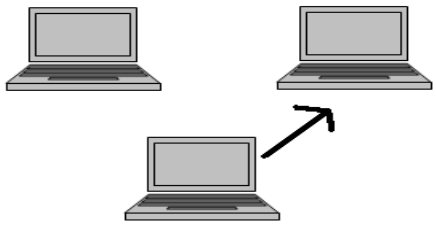
c. Modifikasi (Modification).

Merupakan suatu bentuk ancaman terhadap integritas,dimana pihak yang tidak berhak berhasil mendapat hak akses untuk mengubah suatu data atau informasi dari suatu system computer.biasanya data atau informasi yang diubah adalah record dari suatu tabel pada file database.



Pengiriman Terjadi Modifikasi

d. Pabrifikasi (fabrication),
Merupakan suatu bentuk ancaman terhadap integritas. Tindakan yang biasa dilakukan dengan meniru dan memalsukan suatu objek kedalam system computer.



Pengiriman Terjadi Pabrifikasi

2.4 Program Perusak/Pengganggu

Secara garis besar program yang umumnya merusak atau mengganggu system computer dapat dikelompokan sebagai berikut:

a. **Bug**

Merupakan kesalahan-kesalahan yang terdapat pada suatu program aplikasi yang terjadi secara tidak sengaja.hal ini umumnya dikarenakan kecerobohan dari pihak programmerpada waktu menulis program tersebut.

b. **Chameleons**

Merupakan program yang diseludupkan atau disisipkan kedalam suatu system computer dan berfungsi untuk mencuri data dari system computer yang bersangkutan.

c. **Logic Bomb**

Bomb akan ditempatkan atau dikirimkan secara diam-diam pada suatu system komputeryang menjadi target dan akan meledak biloa pemicunya diaktifkan.

d. **Trojan Horse**

Prinsip kerja dari Trojan horse mirip seperti *chameleons*, bedanya Trojan horse akan melakukan sabotase dan perusakan terhadap system computer yang dijangkitinya.

e. **Virus**

Pada awalnya virus computer merupakan suatu program yang dibuat hanya untuk menampilkan nama samaran serta beberapa baris kata dari pembuatnya, dan sama sekali tidak membahayakan computer.

f. **Worm**

Merupakan suatu program penggangu yang dapat memperbanyak diri dan akan selalu berusaha menyebarkan diri dari satu computer ke computer yang lain dalam suatu jaringan.

2.5 Prinsip Desain Pengamanan

a. Least Privilage.

Prinsip ini menyatakan bahwa setiap proses yang dilakukan pengguna suatu system computer harus beroperasi pada level terendah yang diperlukan untuk menyelesaikan tugasnya.

b. Economy of Mechanism.

Prinsip ini menyatakan bahwa mekanisme keamanan dari suatu system harus sederhana sehingga dapat diverifikasi dan diimplementasi dengan benar.

c. Complete Mediation.

Prinsip ini menyatakan bahwa setiap akses ke system computer harus di cek kedalam informasi kendali akses untuk otorisasi yang tepat.

d. Open Design.

Prinsip ini menyatakan bahwa mekanisme keamanan dari suatu sistemharus dapat diinformasikan dengan baik sehingga memungkinkan adanya umpan balik yang dapat dimanfaatkan untuk perbaikan system keamanan.

e. Separation of Priviledge.

Prinsip ini menyatakan bahwa untuk mengaksessuatu informasi tertentu seorang pengguna harus memenuhi persyaratan tertentu.

f. Least Common Mechanism.

Prinsip ini menyatakan bahwa antar pengguna harus terpisah dalam system.

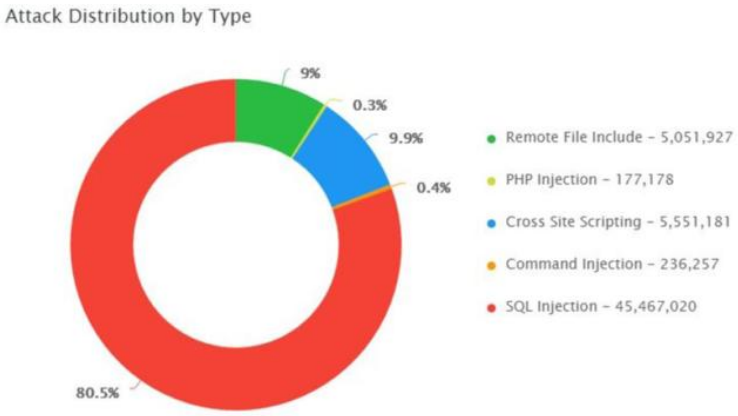
g. Psychological Acceptability.

Prinsip ini menyatakan bahwa mekanisme pengendalian system keamanan harus mudah digunakan oleh pengguna.

C. ANCAMAN KEAMAN KOMPUTER

Serangan pada suatu siswtem jaringan computer sendiri pada dasarnya memiliki tiga gelombang tren utama yaitu:

- Gelombang utama pada serangan fisik .serangan ditujukan kepada fasilitas jaringan,perangkat elektronik,dan computer.
- Gelombang kedua adalah serangan sintaktik.serangan ini ditujukan terhadap kerentanan pada software ,celah yang ada pada algoritma kriptografi atau protocol.
- Gelombang ketiga adalah serangan semantic.serangan jenis ini memanfaatkan arti dari isi pesan yang dikirim.dengan kata lain adalah menyebarkan informasi melalui jaringan,atau menyebarkan informasi tertentu yang mengakibatkan timbulnya suatu kejadian.



Sedangkan mnurut David Icove, berdasarkan lubang atau celah keamanan, keamanan dapat diklasifikasikann menjadi empat yaitu:

a. **Keamanan yang bersifat fisik**: Termasuk akses orang ke gedung,peralatan,dan media yang digunakan.Beberapa bekas penjahat computer mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan.Misalnya pernah diketemukan coretan Password yang di buang tanpa dihancurkan.

b. **Keamanan yang berhubungan dengan orang**: Termasuk identifikikasi,dan profil risiko dari orang yang mempunyai akses

c. **Keamanan dari data dan media serta teknik komunikasi (communication)**. Yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data.seorang criminal dapat memasang virus atau Trojan horse sehingga dapat mengumpulkan informasi yang semestinya tidak berhak di akses.

d. **Keamanan dalam operasi**: Termasuk prosedur yang digunakan untuk mengatur dan mengelola system keamanan,dan juga termasuk prosedur setelah serangan.

3.1 Serangan Lokal

Screen saver password juga dapat di-crack dengan **95scrk***(Screen saver Cracker*).keduanya mudah digunakan dan dapat diperoleh gratis diinternet.Tinggal mengamankan dokumen dengan melindungi folder dan file itu sendiriyang relative lebih sulit dibongkar oleh hacker amatiran.itu pun belum seratus persen aman.
Petunjuk menuliskan kata sandi adalah:

- Jangan dicatat di kertas sebab sangat riskan .simpanlah di tempat tersembunyi.
- Kumpulkan password account untuk email.
- Jangan mudah di tebak.
- Harus mampu melindungi dari tiga serangan: *unauthorized disclosure*, *unauthorized modification* dan *unauthorized removal.*
- Hindari pemakaian kata-kata:nama sendiri atau tanggal ulang tahun.
- Gantilah minimum sebulan sekali.ini sangat berguna bila password berhasil di-crack,maka hacker akan tertipu sebab password telah berubah.
- Apabila pengguna gagal dalam melakukan login jaringan ,bekukan account beberapa saat.

3.2 Bahaya Internet

Bahaya sewaktu berinternet sudah dimulai sewaktu kita berselancar dan dapat dibagi atas dua bagian besar:

- *Remote Contrlled PC*
- Infeksi Digital:virus dan Trojan

a. Remote Controlled PC

Akhir-akhir ini web lebih atraktif dan interaktif karena didesain secara dinamis.komponen-komponen ini selain membuat Web lebih menarik,juga menyimpan potensi bahaya dari penyalahgunaan.ada empat komponen aktif yang sedang marak, yaitu:ActiveX,Java applet,java script,dan VBScript.
Ada beberapa aturan yang harus diikuti oleh suatu program java:

- Hanya mengakses daerah tertentu pada system computer local
- Tidak menjalankan program lian pada computer local
- Dijalankan hanya pada PC yang terhubung ke Internet
- Hanya mengakses system file local atau melakukan pertukaran data melalui jaringan dan tidak bisa keduanya.
- Tidak dapat mengakses memori dari program.

b. Infeksi Digital: Virus dan Trojan

Bahaya terbesar terhadap computer kita tetaplah virus dan Trojan horse.
Dalam praktiknya, terdapat dua opsi untuk menghadapi infeksi virus.

- Usaha pencegahan untuk melindungi computer agar tidak terinfeksi virus.
- Apabila infeksi telah terjadi,maka jalan terbaik adalah mengisolasi inmfeksi ini dan membersihkan PC yang bersangkutan sesegera mungkin.

Dalam usaha pencegahan perlu disadari bahwa satu PC dapat terinfeksi virus sewaktu transfer data.potensi bahaya dating dari:

- Pemakaian media penyimpanan :disket,CD ROM,dan zip drive.kita bertanggung jawab langsung atas pemakaian media penyimpanan.
- Apabila PC kita terhubung via jaringan ke PC lain.
- Orang lain mengunakan PC kita dapat mengakibatkan bahaya,baik disengaja maupun tidak.

3.3 Serangan Hacker

Mengenal Hacker dan Cracker

Cracker adalah seseorang yang masuk ke system orang lain,biasanya di jaringan komnputer.mem-byspass kata sandi atau lisensi program computer,atau sengaja melawan keamanan computer.

Hacker menurut *Eric Raymond* didefinisikan sebagai programmer yang pandai.menurut Raymond ada lima karakteristik yang nenandakan seseorang adalah hacker,yaitu:

- Seseorang yang suka belajar detail dari bahasa pemrograman atau system
- Seseorang yang melakukan pemrograman ,tidak Cuma berteori saja.
- Seseorang yang bisa menghargai,menikmati hasil hacking orang lain.
- Seseorang yang dapat secara cepat belajar pemrograman
- Seseorang yang ahli dalam bahasa pemrograman tertentu atau system tertentu,seperti "*UNIX hacker*"

Cara Kerja Hacker

Untuk memberi gambarantentang keseluruhan proses hacking,dibawah ini disajikan langkah-langkah logisnya,yaitu

1. **Footprinting**. Mencari rincian informasi terhadap system-sistem untuk dijadikan sasaran,mencangkup pencarian informasi dengan mesin pencari,*whois*,dan *DNS zone transfer*
2. **Scanning.**terhadap sasaran tertentu dicari pintu masuk yang paling mungkin digunakan *ping sweep* dan *port scan***.**
3. **Enumeration.** Telah intensif terhadap sasaran,yang mencari *user account* abash,*network resource and share.*
4. **Gaining Acces.** Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran**.**
5. **Escalating Privilege.** Apabila baru mendapatkan user password di tahap sebelumnya,di tahap ini di usahakan mendapat privile admin jaringan dengan *password cracking.*
6. **Pilfering.** Proses pengumpulan informasi dimulai lagi untuk mengidentikfikasimekanisme untuk mendapatkan akses ke *trusted system*.
7. **Covering Tracks.** Begitu control penuh terhadap system diperoleh,maka menutup jejak menjadi prioritas.
8. **Creating Backdoors.** Pintu belakang diciptakan pada berbagai bagian dari system untuk memudahkan masuk kembalike system ini dengan cara membentuk user account palsu.

9. **Denial of Service.** Apabila semua usaha di atas gagal , penyerang dapat melumpuhkan sasaran sebagai usaha terakhir.

Etika

Dalam komuniotas hacker ternyata ada etika dan aturan main yang membedakan antara hacker dan cracker.Ada enam etika yang perlu diresapi seorang hacker:

1. Akses ke computer dan apa pun yang akan mengajarkan kepada kita bagaimana dunia ini berjalan atau bekerja harus dilakukan tanpa batas dan total.
2. Semua informasi harus bebas,tidak disembunyikan.
3. Tidak pernah percaya otoritas percaya pada desentralisasi.
4. Seorang hacker hanya dinilai dari kemampuan hackingnya,bukan criteria buatan seperti gelar,umur,posisi atau suku bangsa.
5. Seorang hacker membuat seni dan keindahan di computer.
6. Komputer dapat mengubah hidup kita menuju lebih baik.

Aturan Main Hacker

Gambaran umum aturan main yang perlu diikutiseorang hacker seperti dijelaskan oleh ***Scorpio,***yaitu:

- Di atas segalanya,hormati pengetahuan dan kebebasan informasi.
- Jangan mengambil keuntungan yang tidak adil dari tindakan hacking.
- Tidak mendistribusikan dan mengumpulkan software bajakan.
- Tidak pernah meng-hack sebuah system untuk mencuri uang.
- Tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan.

Langkah Mengamankan Serangan Hacker

Secara umum ada 6 langkah besar yang mungkin bisa digunakanuntuk mengamankan jaringan dan system computer dari serangan hacker,yaitu:

1. *Membuat komite pengarah keamanan*
   Komite pengarah sangat penting untuk dibentuk agar kebijakan keamanan jaringan dapat diterima oleh semua pihak,agar tidak ada orang terpaksa,merasa tersiksa,merasa aksesnya dibatasi dalam beroperasi di jaringan intranet mereka.
2. Mengumpulkan informasi
   Sebelum kebijakan keamanan jaringan diimplementasikan , ada baiknya proses audit yang lengkap dilakukan.
3. Memperhitungkan risiko
   Risiko dalam rumus sederhana dapat digambarkan sebagai sebagai;

   *Risiko = Nilai Aset * Keretanan * Kemungkinan di eksploit*
4. Membuat solusi
   Pada saat ini sudah cukup banyak solusi yang sifatnya *plug n play* yang terdapat dipasar.akan tetapi ,tidak ada satu program atau solusi yang ampuh untuk semua jenis masalah.
5. Implementasi dan edukasi/pendidikan
   Setelah semua dukungan diperoleh maka proses implementasi dapat dilakukan

6. Terus-menerus menganalisis dan merespons.
   Sistem selalu berkembang, oleh karena itu proses analisis dari prosedur yang dikembangkan harus selalu dilakukan.

Carder (Carding)

Istilah carder cendrung kurang popular dibanding hacker dan cracker.Carder merupakan istilah yang digunakan untuk kejahan kartu kredit yang dilakukan lewat transaksi online.

D. E N K R I P S I

4.1 Konsep Enkripsi

Enkripsi merupakan aspek yang sangat penting dalam komunikasi data melalui computer, sehingga kerahasiaan data tetap terjamin. Enkripsi adalah proses yang mengubah suatu data menjadi kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi berasal dari bahasa Yunani kryptos yang berarti rahasia atau tersembunyi. Sedangkan ilmu yang mempelajari seluk beluk enkripsi dan deksripsi (kebalikan enkripsi) disebut Crytograpby. Orang yang berusaha memecahkan kode enkripsi tanpa kuncinya disebut Cryptoanalyst (hacker).

4.2 Cara kerja enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi, data kita disandikan (encrypted) dengan mengunakan sebuah kunci (key). Untuk membuka (men-decrypt) data tersebut, juga digunakan kunci yang dapat sama dengan kunci untuk mengenkripsi (privat key) atau dengan kunci yang berbeda (public key)

Enkripsi menggunakan semacam algoritma untuk mengubah data atau pesan asli, yang disebut dengan plain text untuk menjadi cipher text, atau bentuk yang terenkripsi. Sebaliknya proses untuk mengubah cipher text menjadi plaintext disebut dekripsi. Misalnya kalimat “I Love You” dengan enkripsi Caesar akan menjadi “loryh brx”. Enkripsi Caesar diambil dari nama Julius Caesar. Aturan dari enkripsi Caesar adalah menggeser huruf sejumlah bilangan tertentu dengan pesan asli sehingga menjadi huruf lain. Pada contoh diatas, tiap-tiap huruf pada pesan asli digeser 3 huruf kekanan.

Keamanan dari enkripsi bergantung pada beberapa factor. Pertama, algoritma enkripsi harus cukup kuat sehingga sulit untuk men-decrypt cipher text dengan dasar cipher text tersebut. Lebih jauh lagi, keamanan dari algoritma enkripsi bergantung pada kerahasiaan dari kuncinya bukan algoritmanya, yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk men-deycrypt informasi dengan dasar chipper text dan pengetahuan tentang algoritma dekripsi atau enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya.

Pada prinsipnya model implementasi kriptografi dalam enkripsi data dibedakan menjadi dua yaitu:

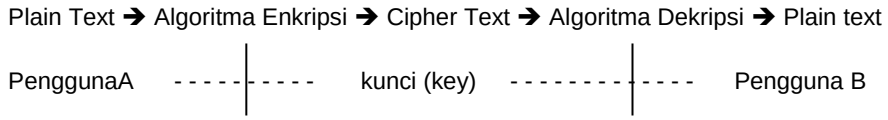
a. Kriptografi dengan enkripsi simetris, yaitu penggunaan kunci (key) yang sama antara saat pengiriman data dan penerimaan data. Algoritma yang digunakan seperti Data Encryption standart (DES), dan Blowfish.
b. Kriptografi dengan enkripsi, yaitu penggunaan kunci (key) yang tidak sama (berlainan) saat pangiriman dan penerimaan. System ini menggunakan dua buah key, yaitu privat key dan public key.

Teknik Enkripsi

Terdapat beberapa teknik enkripsi yang digunakan dalam suatu komunikasi data pada jaringan komputer

Enkripsi Konvensional

Proses enkripsi ini dapat digambarkan sebagai berikut:



Informasi asal yang dapat dimengerti disimbolkan oleh plain text, yang kemudian oleh algoritma enkripsi diterjemahkan menjadi informasi yang tidak dapat dimengerti yang disimbolkan dengan Cipher text. Proses enkripsi terdiri dua yaitu algoritma dan kunci. Kunci biasanya merupakan suatu string bit yang pendek yang mengendalikan algoritma. Algoritma enkripsi akan menghasilkan hasil yang berbeda bergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah output dari algoritma enkripsi. Sekali cipher text telah dihasilkan, kemudian ditransmisikan. Pada bagian penerima selanjutnya cipher text yang diterima diubah kembali ke plain text dengan algoritma dan kunci yang sama.

Keamanan dari enkripsi konvensional bergantung pada beberapa faktor. Pertama algoritma enkripsi harus cukup kuat sehingga menjadikan sangat sulit untuk mendekripsi cipher text tersebut. Lebih dari itu keamanan dari algoritma enkripsi konvensional bergantung pada kerahasiaan dari kuncinya, bukan algoritmanya, yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk mendekripsikan informasi dengan dasar cipher teks dan pengetahuan tentang algoritma dekripsi/ enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya.

Manfaat dari konvensional enkripsi algoritma adalah kemudahan dalam penggunaan secara luas. Dengan kenyataan bahwa algoritma ini tidak perlu dijaga kerahasiaannya dan dengan maksud bahwa pembuat mampu membuat suatu implementasi dalam bentuk chip dengan harga yang murah. Chip ini dapat tersedia secara luas dan disediakan pula untuk beberapa produk. Dengan penggunaan dari enkripsi konvensional, prinsip keamanan adalah menjadi menjaga keamanan dari kunci. Yang dibutuhkan untuk bekerja:

1. Algoritma yang sama dengan kunci yang sama dapat digunakan untuk proses dekripsi-enkripsi.
2. Pengirim dan penerima harus membagi algoritma dan kunci yang sama.

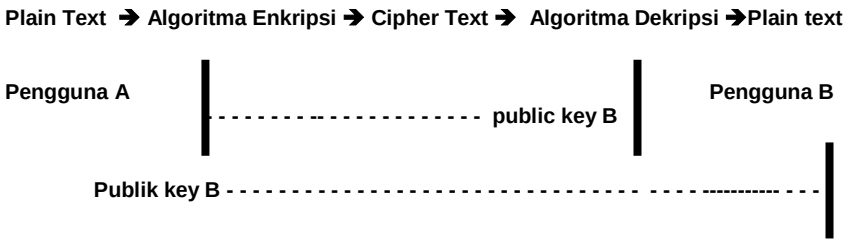
Yang dibutuhkan untuk keamanan:

1. Kunci harus dirahasiakan.
2. Adalah tidak mungkin atau sangat tidak praktis untuk menerjemahkan informasi yang telah dienkripsi.
3. Pengetahuan tentang algoritma dan sample dari kata yang terenkripsi tidak mencukupi untuk menentukan kunci.

Enkripsi Public-key

Salah satu yang menjadi kesulitan utama dari enkripsi konvensional adalah perlunya untuk mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara yang tepat telah diketemukan untuk mengatasi kelemahan ini dengan suatu model enkripsi yang secara mengejutkan tida memerlukan sebuah kunci untuk didistribusikan.

Metode ini dikenal dengan nama enkripsi public-key dan pertama kali diperkenalkan pada tahun 1976.



Algoritma tersebut seperti yang digambarkan. Untuk enkripsi konvensional, kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama. Tetapi ini bukanlah kondisi sesungguhnya yang diperlukan, namun dimungkinkan untuk membangun suatu algoritma yang menggunakan satu kunci untuk enkripsi dan pasangannya, kunci yang berbeda, untuk dekripsi. Lebih jauh lagi, adalah mungkin untuk menciptakan suatu algoritma yang mana pengetahuan tentang algoritma enkripsi ditambah kunci enkripsi tidak cukup untuk menentukan kunci dekripsi, sehingga teknik berikut ini akan dapat dilakukan:

1. Masing-masing dari sistem dalam jaringan akan menciptakan sepasang kunci yang digunakan untuk enkripsi dan dekripsi dari informasi yang diterima.
2. Masing-masing dari system akan menerbitkan kunci enkripsinya kunci public (public key) dengan memasang register umum atau file, sedang pasangannya tetap dijaga sebagai kunci prifat (private key).
3. Jika A ingin mengirim pesan kepada B, maka A akan mengenkripsi pesannya dengan kunci public dari B.
4. Ketika B menerima pesan dari A maka B akan menggunakan kunci privatnya untuk mendiskripsi pesan dari A.

E. KEAMANAN DI INTERNET

5.1 Titik pengamanan

Server Web

Setup dan konfigurasi sebuah server web untuk menyelenggarakan e-commere cukup kompleks, dan akibat dari kesalahan kecil bisa fatal. Contoh: Seorang administrator system mengetahui bahwa untuk proses/program/daemon agar mampu menaggapi permintaan terhadap port tertentu, harus dijalankan dengan hak super user (Root).

Sistem Operasi Jaringan (network Operating System-NOS)

Jika kita terhubung dalam jaringan, maka maka yang harus dilakukan untuk pengamanan adalah:

- Tidak terbagi file maupun folder. Kalau pun kita sering kali berbagi dokumen dengan rekan kerja, sebaiknya gunakan kata sandi.
- Dengan membentengi folder atau file memakai kata sandi dan tidak men-share secara penuh, kemungkinan PC kita tidak diintip orang lain. Untuk mengetahui apakah PC kita diakses orang lain, gunakan beberapa software proteksi dan keamanan yang benyak tersedia dipasaran.
- Windows senenarna sudah dilengkapi dengam utilitas keamanan jaringan, salah satu contohnya adalah Netwatcber. Kita bisa mengetahui orang lain yang berusaha menbuka-buka file atau folder yang kebetulan kita share secara puhuh.

Untuk menghindari hal tersebut, maka perlu melengkapi computer atau jaringan dengan beberapa pengaman, di antaranya:

a. Firewall

Untuk meminimalkan hacker masuk secara jarak jauh. Teliti ketika hendak melakukan file sharing di jaringan, aturlah secara tepat siapa saja pengguna yang berhak mengakses computer kita.

Firewall adalah istilah yang digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan. Firewall dapat berupa solusi hardware dan software yang membatasi akses dan jaringan internal ke internet atau sebaliknya. Firewall dapat juga digunakan untuk memisahkan dua atau lebih jaringan local. Firewall merupakan suatu cara yang efektif untuk melindungi jaringan dari ancaman gangguan lewat intenet. Selain itu firewall dalam jaringan computer membatasi dan menjaga kerusakan pada satu bagian jaringan tidak menyebar ke bagian lain di jaringan.

Firewall mempunyai beberapa tugas:

- Mengimplementasikan kebijakan keamanan dijaringan (site security policy). Jika tindakan tertentu tidak diperbolehkan oleh kibijakan ini, firewall akan menggagalkan operasi tersebut.
- Melakukan filter dengan mewajibkan semua lalu lintas yang ada untuk dilewatkan melalui firewall bagi semua proses pemberian dan pemanfaatan layanan informasi.

- Merekam atau mencatat semua ivent yang mencurigakan atau memberitahu administrator terhadap segala usaha yang menembus kebijakan keamanan.
- Alamat IP asal
- Alamat IP tujuan
- Protokol (TCP, UDP, ICMP)
- Port TCP atau UDP asal
- Port TCP atau UDP tujuan

Sebagai pengaman, firewall tidak sepenuhnya seratus persen dapat melindungi jaringan dari ancaman dan gangguan, seperti di antaranya:

a. Firewall tidak dapat melindungi jaringan dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju jaringan tersebut).
b. Firewall tidak dapat melindungi dari serangan dengan metode baru yang belum dikenalnya
c. Firewall tidak dapat melindungi dari serangan virus.

b. File NTFS,

Yang meningkatkan keamanan secara signifikan dibandingkan dengan system file FAT/FAT32 yang biasa digunakan.

c. Zone Alarm

Yang selain melindungi PC dari akses illegal dalam sebuah jaringan, juga berfungsi sebagai firewall. Kita dapat memiliki koneksi Internet software ini pada www.zone-alarm-pro.com, atau versi yang gratis di www.zdnet.com. Salah satu figurnya yang bagus adalah Trusty IP. Kita bisa memasukkan nomor alamat IP dari teman yang boleh mengakses PC kita.

5.2 Pengamanan Email

Surat Kaleng di Internet

Mungkin akan timbul pertanyaan di benak kita, apakah mengirim e-mail bisa tanpa atau menyembuyikan alamat pengirim, seperti yang bisa dilakukan pengirim surat melalui pos? Jawabnya jelas bisa, kita dapat mengirim anonymous e-mail dengan software seperti Private Idaho dengan menggunakan fasilitas remailer yang ada pada software ini.

Private Idaho dapat di-download di http://www.lynagh.demon.co.uk/pidaho dan untuk menjalankannya diperlukan VBRun 300.dll di C:\Windows\System. Download VBRun 300.dll dapat dilakukan dialamat ini: http://www.bodgres.clara.net/vbrun.htm.

E-mail Bomb

E-mail dapat digunakan untuk melumpuhkan computer yang terhubung ke internet, bahkan seluruh jaringan computer perusahaan dapat dilumpuhkan dengan e-mail bomb.

S/MIME E-mail

Keamanan MIME menggunakan metode enkripsi untuk melindungi e-mail terhadap tiga tipe pelanggaran keamanan yaitu: pengintipan (snopping), pengubahan (tampering), dan pemalsuan (forgery)

S/MIME memanfaatkan (digital signature) (enkripsi dengan kunci private) untuk memproteksi terhadap bahaya pengubah dan pemalsuan. Untuk mengetahui keaslian pengirim, maka digunakan mekanisme sertifikasi dari pihak ketiga, Verisign misalnya.

Implementasi S/MIME E-mail:

- WorldSecure Client
- OpenSoft ExpressMail
- Netscape Messenger

Petunjuk memgirim e-mail secara aman:

1. Memiliki kunci public.
2. Kirim e-mail berisi kunci public ke orang-orang yang kita ingin berkorespodensi dengan mereka menggunakan secure e-mail. Saat e-mail itu tiba di mail client penerima, kunci public kita akan secara otomatis ditambahkan kebuku alamat mail client penerima.
3. Ketika penerima membalas surat, e-mail client miliknya dari buku alamat mengetahui kalau kita mampu bersurat-suratan secara aman. Mail client otomatis akan mengkode e-mail yang akan terkirim tersebut dengan kunci public milik kita.
4. Saat menerima e-mail, mail client kita secara otomatis membongkar penyandian mail terkirim tadi dengan kunci private, sehingga kita bisa membacanya. E-mail yang aman tidak akan dapat terbaca (dibajak) di tengah jalan.

SSL

Secure Socket Layer (SSL) adalah protocol keamanan yang dirancang oleh Netscape Communications Corp. SSL didesain untuk menyediakan keamanan selama transmisi data yang sensitive melalui TCP/IP. SSL menyediakan enkripsi data, autentifikasi server, dan integritas pesan. SSL 2.0 hanya mendukung autentikasi server, sedang SSL 3.0 mendukung uutentikasi client dan server. SSL memenfaatkan kunci public. Data yang dienkripsi dengan kunci public hanya bisa dibuka dengan kunci privat.

Secara teknis operasi SSL adalah:

- Ketika browser mengakses SSL protected page, server SSL mengirim reques ke browser (klient) untuk mengawali sesi yang aman.
- Jika browser mendukung SSL, akan ada jawaban balik yang segera memulai bandsbaking.

Respons dari browser meliputi ID sesi, algoritma enkrepsi, dan metode kompresi.

- Server menetapkan kunci public yang digunakan dalan enkripsi.
- Browser memanfaatkan kunci public untuk mengenkripsi data yang akan ditransmisikannya.

- Server yang menerima data pengiriman akan memakai kunci privat untuk mendeskripsi.

Ciri-ciri Secure Mode adalah

- Di URL muncul tulisan https:// bukan lagi http://
- Di Netscape Navigator (versi 3.0 dan sebelumnya) simbul kunci patah yang ada di sudut kiri layer menjadi kunci yang utuh menyambung. Di Netscape Communicator 4.0, kunci gembok yang tadinya terbuka menjadi tertutup. Di Microsoft Internet Explorer, muncul tanda kunci di bagian bawah browser.

Enkripsi E-mail

Kerahasiaan e-mail bisa terancam dari siapa saja baik dari pihak luar atau dalam organisasi kita sendiri seperti para administrator system.

- Enkripsi Simatrik. Ada dua macam enkripsi, cenkripsi simetrik (symmetric encryption) dan enkripsi asemetrik (asymmetric encryption). Pada enkripsi simetrik, pada pengiriman dan penerimaan menggunakan kunci yang sama (simatrik).
- Enkripsi asemetrik. Untuk mengatasi masalah pengiriman kunci seperti yang terdapat pada enkripsi simetrik, dikembangkan enkripsi asemetrik (asymmetric encryption), yang disini kedua belah pihak memegang dari satu pasangan kunci. Personal key hanya untuk pemakaian sendiri dan harus tetap rahasia dan tidak diberikan kepada orang lain. Kunci ini dapat meng-enkripsi dan mendekripsi pesan yang dienkripsi dengan kunci public. Kunci public ditujukan untuk didistribusikan pada rekan komunikasi dari pemegang kunci privat. Kunci public akan digunakan untuk mengirimkan pesan terenkripsi yang hanya dapat dibuka menggunakan kunci privat.
- Enkripsi Personal (Personal Encryption). Kriptografi yang mudah digunakan namun tangguh baru ada semenjak Pbil Zimmerman memperkenalkan programnya, PGP (Pretty Good Privacy) pada tahun 1991.
- Steganografi. Berbeda dengan PGP yang mengenkripsi file menjadi teks acak, maka steganografi meng-enkripsi teks dengan menyembunyikan pada file gambar atau suara. Steganografi adalah salah satu jenis enkripsi yang menggunakan kunci simetrik (symmetric key).

5.3 Tanda Tangan dan Sertifikat Digital

Tanda tangan digital adalah tanda tangan yang dilakukan secara elektronik untuk kepentingan transaksi digital, seperti e-banking dan e-commerce. Teknologi tersebut memanfaatkan teknilogi kunci public. Sepasang kunci public-privat dibuat untuk keperluan seorang. Kunci privat disimpan oleh pemiliknya dan dipergunakan untuk membuat tanda tangan digital. Sedangkan kunci public dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu document.

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah

1. Tanda tangan itu asli (autentik), tidak mudah ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatanganan tidak bisa menyangkal bahwa ia dulu tidak pernah menandatanganinya.
2. Tanda tangan itu hanya sah untuk dokumen (pesan)itu saja. Tanda tangan itu tidak bisa dipindahkan dari dokumen lainnya. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
3. Tanda tangan itu dapat diperiksa dengan mudah.
4. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
5. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

F. PEMELIHARAAN SISTEM KOMPUTER

Proses pmeliharaan biasanya dilakukan sebelum perangkat atau data digunakan terjadi permasalahan. Artinya bahwa pemeliharaan dilakukan dalam sebagai preventif atau pencegahan dalam sebuah operasikomputer untuk menghadapi sebuah risiko yang mungkin akan terjadi.

Perawatan terrencana dilakukan dengan mendata:

- Jenis dan fugsi komputer
- Komponen-komponen yang dimiliki komputer
- Lama computer saat digunakan
- Jumlah computer yang akan dilakukan perawatan

Perawatan terencana dilakukan menjadi tiga jenis perawataan yaitu:

1 Preventif, yaitu jenis perawataan yang dilakukan untuk mencagah terjadinya berbagai kemungkinan kerusakan pada sistem komputer. Tidak preventif tentunya dilakukan sebelum computer mengalami masalah atau kerusakan.

2 Prediktif, yaitu jenis perawatan yang dilakukan karena adanya praduga terhadap sebuah alat atau komponen yang sebenarnya masih berfungsi dengan baik namun diperkirakantidak lagi bertahan sampai dengan pelaksanaan perawatan preventif pada tahap berikutnya.

3 Korektif, yaitu tindakan perawataan yang difokuskan terhadap pemeriksaan fungsi dari bagian-bagian utama mesin komputer atau *overbold*.

Untuk menjaga kinerja system komputer kita tersebut,maka perlu dilakukan langkah-langkah sebagai berikut:

6.1 Melakukan *update* program antivirus secara berkala

Saat ini banyak jenis variasi virus yang beredar ,kebanyakan diantaranya dapat dikelompokkan menjadi enam kategori umum, dimana tiap jenis sedikit berbeda cara kerjanya.

- Virus boot-sector. Mengganti atau memasukkan boot-sector sebuah area pada hard drive (atau jenis disk lainnya) yang akan diakses pertama kali saat computer dinyalakan. Virus jenis ini dapat menghalangi computer untuk melakukan booting dari hard disk.
- Virus file. Menginfeksi aplikasi. Virus ini melakukan eksekusi untuk menyebarkan dirinya pada aplikasi dan dokumen yang terkait dengannya saat file yang terinfeksi dibuka atau dijalankan.
- Virus makro. Ditulis dengan menggunakan bahasa pemrograman makro yang disederhanakan, dan menginfeksi aplikasi Microsoft Office, seperti Word dan Exel, dan saat ini diperkirakan 75 persen dari jenis virus ini telah tersebar di dunia. Sebuah dokumen yang terinfeksi oleh virus makro secara umum akan memodifikasi perintah yang telah ada dan digunakan (seperti perintah “save”) untuk memicu penyebaran dirinya saat perintah tersebut dijalankan.

- Virus multipartite. Menginfeksi baik file dan boot-sector, penjahat berkedok ganda yang dapat menginfeksi system terus-menerus sebelum ditangkap oleh scanner antivirus.
- Virus polymorphic. Akan mengubah kode dirinya saat dilewatkan pada mesin yang berbeda; secara teoretis virus jenis ini susah untuk dapat dideteksi oleh scanner anti virus, tetapi dalam kenyataannya jenis virus ini tidak ditulis dengan baik, sehingga mudah untuk diketahui keberadaannya.
- Virus stealth. Menyembunyikan dirinya dengan membuat file yang terinfeksi tampak tidak terinfeksi, tetapi virus jenis ini jarang mampu menghadapi scanner antivirus terbaru.

Indikasi adanya virus pada computer dapat dilihat pada penjelasan berikut:

- Penambahan ukuran file tanpa alas an yang jelas. Hal ini mengidentifikasikan adanya virus.
- Program tidak berjalan secara normal dan ddengan pesan-pesan error. Atau adakalanya disertai dengan animasi-animasi (walaupun menarik).
- Adanya perubahan-perubahan struktur direktori tanpa sebab.
- Penurunan jumlah memori yang tersedia yang disebabkan bukan karena computer sedang menjalankan program-program computer.
- Aktivitas system keseluruhan berjalan secara lambat. Untuk mengeksekusi program membutuhkan waktu yang lebih lama dari biasanya.

Sedangkan cara mencegah dan menanggulangi virus masuk ke sistem computer adalah sebagai berikut:

- Mengetahui dengan pasti apakah file atau program yang akan dikirim melalui e-mail tersebut mengandung virus atau tidak.
- Mengetahui dan memastikan attachment e-mail tersebut dari siapa, sebelu disimpan atau dijalankan.
- Memastikan bahwa kita telah menanti attachment e-mail dari seorang yang kita kenal dan percayai.
- Menginstalasi software anti virus sekarang pada system computer. Vendor software anti virus besar, seperti Symantec, network associates, computer associates, dan kapersky lab, menyediakan layanan update regular (sebagai catatan computer associates inoculate IT merupakan software anti virus yang gratis). Beberapa vendor juga menawarkan layanan update regular melalui situs web perusahaan mereka.
- Update secara regular sangat penting. Para periset dari computer economics memperkirakan bahwa 30 persen dari usah kecil sangat rentan terhadap bahaya virus dan itu dikarenakan mereka tidak meng-update software anti virus mereka secara teratur, atau mereka tidak menginstalasikannya secara benar.
- Mempunyai computer back-up (cadangan) untuk menyimpan data penting. Jika tidak punya data back-up, miliki zip drive dan rutin selalu untuk mem-backup data file tersebut.

- Jika ragu-ragu, hapus beberapa pesan e-mail atau attachment yang mencurigakan dan kirim e-mail kepada pengirim untuk memberitahu bahwa kita mencurigai suatu virus.
- Jangan pernah untuk membuka sebuah lampiran dengan ektensi file: EXE, COM, VBS, LNK,PIF, SCR, BAT.

Beberapa langkah dapat kita lakukan untuk menghindarkan system dari ancaman virus maupun akibat-akibat buruk yang ditimbulkan. Langkah-langkah tersebut antara lain:

- Pasang anti virus pada system kita. Sebagai perlindungan digari depan, penggunaan anti virus adalah wajib. Ada banyak anti virus yang beredar dipasaran saat ini. Beberapa yang cukup handal diantaranya adalah McAfree virus scan (www.mcafee.com) dan Norton anti viru (www.symantec.com), PCC illin , panda anti virus, dan Norman anti virus. Dapat juga digunakan versi freeware seperti AVG anti virus dan anti vir.
- Update database program anti virus secara teratur. Ratusan virus baru muncul setiap bulannya. Usahakan untuk selalu meng-update database dari program anti virus yang kita gunakan. Database terbaru dapat dilihat pada situs web perusahaan pembuat program anti virus yang digunakan.
- Berhati-hati sebelum menjalankan file baru. Lakukan sccaning terlebih dahulu dengan antivirus sebelum menjalankan sebuah file yang didapat dari men-download di internet atau mengopy dari orang lain. Apabila kita bisa menggunakan sarana e-mail, berhati-hatilah setiap menerima attachment dalam bentuk file executable. Waspadai file-file yang berektensi: *.COM, *.EXE, *.VBS, *. SCR, *.VB. Jangan terkecoh untuk langsung membukanya sebelu melakukan sccaning dengan software anti virus.
- Curigai apabila terjadi keanehan pada system kita.Menurunnya kinerja system secara drastis, khususnya pada saat melakukan operasi pembacaan/penulisan file di disk, serta munculnya masalah pada software saat dioperasikan bisa jadi merupakan indikasi bahwa system telah terinfeksi oleh viru. Berhati-hatilah!
- Back up data kita secara teratur. Tips ini mungkin tidak secara langsung menyelamatkan data kita dari ancaman virus, namun demikian akan sangat berguna apabila suatu saat virus betul-betul menyerang dan merusak data di computer yang digunakan. Setidaknya dalam kondisi tersebut, kita tidak akan kehilangan seluruh data yang telah kita back up sebelumnya.

6.2 Backup Data

Pemeliharaan computer yang paling sering bahkan ruti dilakukan adalah dengan cara backup data (membuat cadangan data) yaitu dengan cara mengopy atau menggandakan data pada tempat tertentu. Agar data yang di-backup mempunyai arti penting dalam sebuah dokumentasi, maka hal yang penting bagi kita adalah dengan cara membuat strategi backup data untuk mencegah lenyapnya data dari computer.

Media Backup

- Disket. Backup data dengan disket sifatnya biasanya dikatakan sementara,karene sifat penyimpanannya yang tidak tahan lama,sehingga kurang begitu tepat untuk melakukan backup data untuk jangka waktu yang lama.
- Hard disk. Jika kita memiliki lebih dari satu hard disk, ini adalah cara backup data yang paling bisa dilakukan;cepat dan murah(tidak perlu membeli peralatan).Kumpulkan seluruh data disebuah direktoridi hard disk pertama, dan secara rutin duplikasi direktori tersebut ke hard disk kedua.Kekurangannya,data Kita masih tetap terkumpul dikomputer yang sama,jadi masalah seperti *surge/spike*(lonjakan arus listrik)sangat mungkin akan merusakkan hard disk tersebut secara bersamaan.
- CD-R (CD Recordable)
- Zip drive. Kelebihan Zip Drive adalah cukup untuk mem-backup data, dan harga drive cukup murah sekarang.
- Stik Memori drive. Kelebihannya,perangkat ini sangat praktis,bentuknya hanya sebesar jari tangan,kecepatan baca data untuk backup sangat cepat karena menggunakan *port* antar muka USB,bisa menyimpan data sampai kapasitas Giga Byte.
- QIC tape drive. Kelebihannya,harga drive lebih murah disbanding DLT drive,harga *cartridge* juga lebih murah, bisa back data via port parallel saja.Kekurangannya,kapasitas tidak besar DLT (maksimum pada saat artikel ini ditulis adalah 30 GB),kecepatan backup sangat lambat,kadanh tidak bisa diandalkan.
- DLT tape drive.Kelebihannya,sangat capat dalam mem-backup data,kapasitas sangat besar,dapat diandalkan.Kekurangannya,harga SANGAT mahal (biasanya sampai ribuan dolar AS).
- Internet. Ini alternatif baru yang mungkin bisa dilakukan, berkat munculnya berbagai Web yang menyediakan jasa penyimpanan data secara cuma-cuma di Internet.

Referensi Utama

1. *Andrew S. Tanembaum, Structure Computer Organization, Fourth Edition, Prentice-Hall,*
2. *Gordon B. Davis, Computer Data Processing, Second Edition, New York McGraw-Hill Book Company*
3. *James D. Shoeffler, Minicomputers: Hardware, Software, and Aplications, The Institute Of Electrical And Engineers, Inc, New York,*

Referensi Pendukung

1. *Gordon B. Davis, Management Information Syastems, Conceptual Foundatioan, Structure, and Development, Second Edition, New York McGraw-Hill Book Company*