KEAMANAN KOMPUTER

Mengapa Keamanan Komputer Sangat Dibutuhkan ?

Information Based Society menyebabkan informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara tepat dan akurat menjadi sangat esensial bagi sebuah organisasi.

Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, namun disisi lain membuka potensi adanya lubang keamanan (security hole) karena jaringan internet bersifat publik.

Menurut Budi Rahardjo, Ph.D., Pakar tehnologi informasi yang menekuni bidang mikroelektronika dan Dosen ITB, sebagaimana di publikasikan pada intelijen.co.id, dalam banyak kasus bobolnya situs-situs lembaga pemerintahan ataupun situs-situs personal tokoh-tokoh penting, bukan karena kecanggihan orang yang meng-*hack*, siapapun dan apapun motifnya. Hal itu terjadi karena lemahnya sistem keamanan tehnologi informasi yang ada.

Meskipun sering terlihat sebagai besaran yang tidak dapat langsung diukur dengan uang (*intangible*), keamanan sebuah sistem informasi sebetulnya dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible*). Dengan adanya ukuran yang terlihat, mudah-mudahan pihak management dapat mengerti pentingnya investasi di bidang keamanan.

Berikut ini adalah berapa contoh kerugian yang timbul akibat kurangnya penerapan keamanan :

- Hitung kerugian apabila sistem informasi anda tidak bekerja selama 1jam, selama 1 hari, 1 minggu, dan 1 bulan. (Sebagai perbandingkan, bayangkan jika server Amazon.com tidak dapat diakses selama beberapa hari. Setiap harinya dia dapat menderita kerugian beberapa juta dolar.)
- Hitung kerugian apabila ada kesalahan informasi (data) pada sistem informasi anda. Misalnya web site anda mengumumkan harga sebuah barang yang berbeda dengan harga yang ada di toko anda.
- Hitung kerugian apabila ada data yang hilang, misalnya berapa kerugian yang diderita apabila daftar pelanggan dan invoice hilang dari sistem anda. Berapa biaya yang dibutuhkan untuk rekonstruksi data.
- Apakah nama baik perusahaan anda merupakan sebuah hal yang harus dilindungi? Bayangkan bila sebuah bank terkenal dengan rentannya pengamanan data-datanya, bolak-balik terjadi security incidents. Tentunya banyak nasabah yang pindah ke bank lain karena takut akan keamanan uangnya.

Keamanan sistem dimaksudkan untuk mencapai tiga tujuan utama yaitu; kerahasiaan, ketersediaan dan integritas.

1. Kerahasian. Setiap organisasi berusaha melindungi data dan informasinya dari pengungkapan kepada pihak-pihak yang tidak berwenang. Sistem informasi yang perlu mendapatkan prioritas kerahasian yang tinggi mencakup; sistem informasi eksekutif, sistem informasi kepagawaian (SDM), sistem informasi keuangan, dan sistem informasi pemanfaatan sumberdaya alam.
2. Ketersediaan. Sistem dimaksudkan untuk selalu siap menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya. Tujuan ini penting khususnya bagi sistem yang berorientasi informasi seperti SIM, DSS dan sistem pakar (ES).
3. Integritas. Semua sistem dan subsistem yang dibangun harus mampu memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya.

Keamanan Menurut Para Ahli

1. Menurut David Icove
   Berdasarkan lubang kemanan, keamanan komputer dapat dibagi menjadi 4 macam, yaitu :
   1) Keamanan Fisik (Physical Security), termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
      Contoh : Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
   2) Denial Of Service, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
   3) Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (hang).
   4) Keamanan yang berhubungan dengan orang
      Contoh :
      - Identifikasi user (username dan password)
      - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
      - Keamanan dari data dan media serta teknik komunikasi
      - Keamanan dalam operasi : Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan
      - juga ter-masuk prosedur setelah serangan (post attack recovery).
2. 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.
   Keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi.

Karakteristik Penyusup :

1. The Curious (Si Ingin Tahu) – tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
2. The Malicious (Si Perusak) – tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
3. The High-Profile Intruder (Si Profil Tinggi) – tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
4. The Competition (Si Pesaing) – tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

- Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- Lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- Wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.

- Larva (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
- Hacker ; aktivitas hacking sebagai profesi.
- Wizard ; hacker yang membuat komunitas pembelajaran di antara mereka.
- Guru ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

Aspek Keamanan Komputer

1. **Privacy** yaitu menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat. Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
2. **Confidentiality** yaitu berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya. Bentuk Serangan : usaha penyadapan (dengan program sniffer). Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.
3. **Integrity** yaitu informasi tidak boleh diubah tanpa seijin pemilik informasi. Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.
4. **Authentication** yaitu metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Dukungan : Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarkingb (untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.
5. **Access control**, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.
6. **Availability** yaitu berhubungan dengan ketersediaan informasi ketika dibutuhkan. Contoh hambatan : “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
7. **Mailbomb**, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.
8. **Access Control** yaitu cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy. Metode : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.
9. **Non Repudiation** yaitu Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Model – Model Penyerangan Keamanan Komputer

Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings ada beberapa kemungkinan serangan (attack):

- Interruption : Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah "denial of service attack".
- Interception : Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).
- Modification : Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- Fabrication : Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Sumber Lubang Keamanan

Lubang keamanan (*security hole*) dapat terjadi karena beberapa hal; salah disain (*design flaw*), salah implementasi, salah konfigurasi, dan salah penggunaan.

- **Salah Disain**, Lubang keamanan yang ditimbulkan oleh salah disain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.
- **Implementasi kurang baik**, Lubang keamanan yang disebabkan oleh kesalahan implementasi sering terjadi. Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibatnya cek atau testing yang harus dilakukan menjadi tidak dilakukan. Lubang keamanan yang terjadi karena masalah ini sudah sangat banyak, dan yang mengherankan terus.terjadi, seolah-olah para programmer tidak belajar dari pengalaman
- **Salah konfigurasi**, Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena salah konfigurasi. Contoh masalah yang disebabkan oleh salah konfigurasi adalah berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "*writeable*". Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan.
- **Salah menggunakan program atau sistem**, Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan. Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal. Sering terjadi cerita horor dari sistem administrator baru yang teledor dalam menjalankan perintah "rm -rf" di sistem UNIX (yang menghapus berkas atau direktori beserta sub direktori di dalamnya). Akibatnya seluruh berkas di sistem menjadi hilang mengakibatkan *Denial of Service* (DoS). Apabila sistem yang digunakan ini digunakan bersama-sama, maka akibatnya dapat lebih fatal lagi. Untuk itu perlu berhati-hati dalam menjalan program, terutama apabila dilakukan dengan menggunakan account administrator seperti *root* tersebut.

Mengamankan Sistem Informasi

- **Mengatur Akses (Access Control)**

  Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "authentication" dan "access control". Implementasi dari mekanisme ini antara lain dengan menggunakan "password". Apabila password valid, pemakai yang bersangkutan diperbolehkan menggunakan sistem. Apabila ada yang salah, pemakai tidak dapat menggunakan sistem. Informasi tentang kesalahan ini biasanya dicatat dalam berkas *log*. Besarnya informasi yang dicatat bergantung kepada konfigurasi dari sistem setempat. Misalnya, ada yang menuliskan informasi apabila pemakai memasukkan *user id* dan *password* yang salah sebanyak tiga kali. Ada juga yang langsung menuliskan informasi ke dalam berkas *log* meskipun baru satu kali salah. Informasi tentang waktu kejadian juga dicatat. Selain itu asal hubungan (*connection*) juga dicatat sehingga administrator dapat memeriksa keabsahan hubungan.

  Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai dalam "group". Ada group yang berstatus pemakai biasa, ada tamu, dan ada juga *administrator* atau *super user* yang memiliki kemampuan lebih dari group lainnya.

  Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem anda. Di lingkungan kampus mungkin ada kelompok mahasiswa, staf, karyawan, dan administrator. Sementara itu di lingkungan bisnis mungkin ada kelompok *finance*, *engineer*, *marketing*, dan seterusnya.

- **Menutup servis yang tidak digunakan** Seringkali sistem (perangkat keras dan/atau perangkat lunak) diberikan dengan beberapa servis dijalankan sebagai default. Untuk mengamankan sistem, servis yang tidak diperlukan di server (komputer) tersebut sebaiknya dimatikan.

- **Memasang Proteksi** untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah firewall. Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi yang bersangkutan yang dapat dibagi menjadi dua jenis:

  Ø Apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibitted*)
  Ø Apa-apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*)

  Satu hal yang perlu diingat bahwa adanya firewall bukan menjadi jaminan bahwa jaringan dapat diamankan seratus persen. Intinya adalah bahwa meskipun sudah menggunakan firewall, keamanan harus tetap dipantau secara berkala.

- **Pemantau adanya serangan** Sistem pemantau (monitoring sistem) digunakan untuk mengetahui adanya tamu tak diundang (intruder) atau adanya serangan (attack). Nama lain dari sistem ini adalah "intruder detection sistem" (IDS). Sistem ini dapat memberitahu administrator melalui e-mail maupun melalui mekanisme lain.

- **Backup secara rutin** Seringkali tamu tak diundang (intruder) masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang dapat ditemui. Jika intruder ini berhasil menjebol sistem dan masuk sebagai super user (administrator), maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya backup yang dilakukan secara rutin merupakan sebuah hal yang esensial. Bayangkan apabila yang dihapus oleh tamu ini adalah berkas penting yang sangat rahasia bagi perusahaan.
- **Investment dan personel khusus untuk menangani keamanan**
- **Secara berkala melakukan monitor integritas sistem dengan Cops, tripwire, SATAN, dll.**
- **Audit: rajin baca dan proses log**

Sumber :

http://www.intelijen.co.id/wawancara/1671-budi-rahardjo-indonesia-perlu-pusat-koordinasi-keamanan-ti

budi.insan.co.id/presentation/nii-security.PPT

http://tyobee.blogspot.com/2010/11/keamanan-komputer-menurut-para-ahli.html