

KEAMANAN INFORMASI

Pendahuluan

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayangnya masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi.

Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Bab ini diharapkan dapat memberikan gambaran dan informasi menyeluruh tentang keamanan sistem informasi dan dapat membantu para pemilik dan pengelola sistem informasi dalam mengamankan informasinya.

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).

Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Dahulu, jumlah komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya classified baru dilakukan di sekitar tahun 1950-an.

Pendahuluan

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi.

Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam development, algoritma-algoritma dan teknik-teknik yang digunakan untuk menghasilkan produk tersebut.

Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Pendahuluan

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.

Pendahuluan

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 DAN MANAGEMENT PERUSAHAAN

Seringkali sulit untuk membujuk management perusahaan atau pemilik sistem informasi untuk melakukan investasi di bidang keamanan.

Di tahun 1997 majalah Information Week melakukan survey terhadap 1271 *system* atau *network manager* di Amerika Serikat. Hanya 22% yang menganggap keamanan sistem informasi sebagai komponen sangat penting (“*extremely important*”).

Mereka lebih mementingkan “*reducing cost*” dan “*improving competitiveness*” meskipun perbaikan sistem informasi setelah dirusak justru dapat menelan biaya yang lebih banyak.



KEAMANAN DAN MANAGEMENT PERUSAHAAN

Keamanan itu tidak dapat muncul demikian saja. Dia harus direncanakan. Ambil contoh berikut. Jika kita membangun sebuah rumah, maka pintu rumah kita harus dilengkapi dengan kunci pintu. Jika kita terlupa memasukkan kunci pintu pada budget perencanaan rumah, maka kita akan dikagetkan bahwa ternyata harus keluar dana untuk menjaga keamanan. Kalau rumah kita hanya memiliki satu atau dua pintu, mungkin dampak dari budget tidak seberapa. Bayangkan bila kita mendesain sebuah hotel dengan 200 kamar dan lupa membudgetkan kunci pintu. Dampaknya sangat besar. Demikian pula di sisi pengamanan sebuah sistem informasi. Jika tidak kita budgetkan di awal, kita akan dikagetkan dengan kebutuhan akan adanya perangkat pengamanan (firewall, Intrusion Detection System, anti virus, Disaster Recovery Center, dan seterusnya).

KEAMANAN DAN MANAGEMENT PERUSAHAAN

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.



KEAMANAN DAN MANAGEMENT PERUSAHAAN

Berikut ini adalah beberapa contoh kegiatan yang dapat anda lakukan:

- Hitung kerugian apabila sistem informasi anda tidak bekerja selama 1 jam, selama 1 hari, 1 minggu, dan 1 bulan. (Sebagai perbandingan, 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.

KEAMANAN DAN MANAGEMENT PERUSAHAAN

Berikut ini adalah beberapa contoh kegiatan yang dapat anda lakukan:

- 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 DAN MANAGEMENT PERUSAHAAN

Berikut ini adalah beberapa contoh kegiatan yang dapat anda lakukan:

- 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 DAN MANAGEMENT PERUSAHAAN

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*.




KEAMANAN DAN MANAGEMENT PERUSAHAAN

TABLE 1. Kontribusi terhadap Risk

Nama komponen	Contoh dan keterangan lebih lanjut
Assets (aset)	<ul style="list-style-type: none">• hardware• software• dokumentasi• data• komunikasi• lingkungan• manusia
Threats (ancaman)	<ul style="list-style-type: none">• pemakai (users)• teroris• kecelakaan (accidents)• crackers• penjahat kriminal• nasib (acts of God)• intel luar negeri (foreign intelligence)
Vulnerabilities (kelemahan)	<ul style="list-style-type: none">• software bugs• hardware bugs• radiasi (dari layar, transmisi)• tapping, crosstalk• unauthorized users• cetakan, hardcopy atau print out• keteledoran (oversight)• cracker via telepon• storage media

KEAMANAN DAN MANAGEMENT PERUSAHAAN

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

- usaha untuk mengurangi *Threat*
 - usaha untuk mengurangi *Vulnerability*
 - usaha untuk mengurangi dampak (*impact*)
 - mendeteksi kejadian yang tidak bersahabat (*hostile event*)
 - kembali (*recover*) dari kejadian
- 

BEBERAPA STATISTIK SISTEM KEAMANAN

Ada beberapa statistik yang berhubungan dengan keamanan sistem informasi yang dapat ditampilkan di sini. Data-data yang ditampilkan umumnya bersifat konservatif mengingat banyak perusahaan yang tidak ingin diketahui telah mengalami “security breach” dikarenakan informasi ini dapat menyebabkan “negative publicity”.

Perusahaan-perusahaan tersebut memilih untuk diam dan mencoba menangani sendiri masalah keamanannya tanpa publikasi.

- Tahun 1996, *U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 “insiden” di sistem komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan.

BEBERAPA STATISTIK SISTEM KEAMANAN

- Juga di tahun 1996, *FBI National Computer Crimes Squad*, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan.
- Sebuah penelitian di tahun 1997 yang dilakukan oleh perusahaan *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
- Penelitian di tahun 1996 oleh American Bar Association menunjukkan bahwa dari 1000 perusahaan, 48% telah mengalami “computer fraud” dalam kurun lima tahun terakhir.

BEBERAPA STATISTIK SISTEM KEAMANAN

- Di Inggris, 1996 *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Survey ini juga menunjukkan bahwa kerugian yang diderita rata-rata US \$30.000 untuk setiap insiden. Ditunjukkan juga beberapa organisasi yang mengalami kerugian sampai US \$1.5 juta.
- FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti (*convicted*) di pengadilan naik 88% dari 16 ke 30 kasus.

BEBERAPA STATISTIK SISTEM KEAMANAN

- John Howard dalam penelitiannya di CERT yang berlokasi di Carnegie Mellon University mengamati insiden di Internet yang berlangsung selama kurun waktu 1989 sampai dengan 1995. Hasil penelitiannya antara lain bahwa setiap domain akan mengalami insiden sekali dalam satu tahun dan sebuah komputer (host) akan mengalami insiden sekali dalam 45 tahun.
- Winter 1999, *Computer Security Institute* dan FBI melakukan survey yang kemudian hasilnya diterbitkan dalam laporannya. Dalam laporan ini terdapat bermacam-macam statistik yang menarik, antara lain bahwa 62% responden merasa bahwa pada 12 bulan terakhir ini ada penggunaan sistem komputer yang tidak semestinya (unauthorized use), 57% merasa bahwa hubungan ke Internet merupakan sumber serangan, dan 86% merasa kemungkinan serangan dari dalam (disgruntled employees) dibandingkan dengan 74% yang merasa serangan dari hackers.

BEBERAPA STATISTIK SISTEM KEAMANAN

- Jumlah kelemahan (*vulnerabilities*) sistem informasi yang dilaporkan ke Bugtraq meningkat empat kali (*quadruple*) semenjak tahun 1998 sampai dengan tahun 2000. Pada mulanya ada sekitar 20 laporan menjadi 80 setiap bulannya.
- Pada tahun 1999 CVE2 (*Common Vulnerabilities and Exposure*) mempublikasikan lebih dari 1000 kelemahan sistem. CVE terdiri dari 20 organisasi security (termasuk di dalamnya perusahaan security dan institusi pendidikan).
- Juli 2001 muncul virus *SirCam* dan worm *Code Red* (dan kemudian *Nimda*) yang berdampak pada habisnya bandwidth. Virus *SirCam* mengirimkan file-file dari disk korban (beserta virus juga) ke orang-orang yang pernah mengirim email ke korban. Akibatnya file-file rahasia korban dapat terkirim tanpa diketahui oleh korban.

BEBERAPA STATISTIK SISTEM KEAMANAN

Di sisi lain, orang yang dikirim email ini dapat terinfeksi virus SirCam ini dan juga merasa “dibom” dengan email yang besar-besar. Sebagai contoh, seorang kawan penulis mendapat “bom” email dari korban virus SirCam sebanyak ratusan email (total lebih dari 70 MBytes). Sementara itu worm Code Red menyerang server Microsoft IIS yang mengaktifkan servis tertentu (indexing). Setelah berhasil masuk, worm ini akan melakukan scanning terhadap jaringan untuk mendeteksi apakah ada server yang bisa dimasuki oleh worm ini. Jika ada, maka worm dikirim ke server target tersebut. Di server target yang sudah terinfeksi tersebut terjadi proses scanning kembali dan berulang. Akibatnya jaringan habis untuk saling scanning dan mengirimkan worm ini. Dua buah securityhole ini dieksploit pada saat yang hampir bersamaan sehingga beban jaringan menjadi lebih berat.

BEBERAPA STATISTIK SISTEM KEAMANAN

Jebolnya sistem keamanan tentunya membawa dampak. Ada beberapa contoh akibat dari jebolnya sistem keamanan, antara lain:

- 1988. Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai “*denial of service attack*”. Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar \$100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda \$10.000.

BEBERAPA STATISTIK SISTEM KEAMANAN

Jebolnya sistem keamanan tentunya membawa dampak. Ada beberapa contoh akibat dari jebolnya sistem keamanan, antara lain:

- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport lokal (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts. <http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv> <http://www.news.com/News/Item/0,4,20226,00.html>

BEBERAPA STATISTIK SISTEM KEAMANAN

Jebolnya sistem keamanan tentunya membawa dampak. Ada beberapa contoh akibat dari jebolnya sistem keamanan, antara lain:

- 7 Februari 2000 (Senin) sampai dengan Rabu pagi, 9 Februari 2000. Beberapa web terkemuka di dunia diserang oleh “*distributed denial of service attack*” (DDoS attack) sehingga tidak dapat memberikan layanan (down) selama beberapa jam. Tempat yang diserang antara lain: Yahoo!, Buy.com, eBay, CNN, Amazon.com, ZDNet, E-Trade. FBI mengeluarkan tools untuk mencari program TRINOO atau Tribal Flood Net (TFN) yang diduga digunakan untuk melakukan serangan dari berbagai penjuru dunia.

BEBERAPA STATISTIK SISTEM KEAMANAN

Jebolnya sistem keamanan tentunya membawa dampak. Ada beberapa contoh akibat dari jebolnya sistem keamanan, antara lain:

- 4 Mei 2001. Situs Gibson Research Corp. (grc.com) diserang Denial of Service attack oleh anak berusia 13 tahun sehingga bandwidth dari grc.com yang terdiri dari dua (2) T1 connection menjadi habis. Steve Gibson kemudian meneliti software yang digunakan untuk menyerang (DoS bot, SubSeven trojan), channel yang digunakan untuk berkomunikasi (via IRC), dan akhirnya menemukan beberapa hal tentang DoS attack ini. Informasi lengkapnya ada di situs www.grc.com.
- Juni 2001. Peneliti di UC Berkeley dan University of Maryland berhasil menyadap data-data yang berada pada jaringan wireless LAN (IEEE 802.11b) yang mulai marak digunakan oleh perusahaan-perusahaan

BEBERAPA STATISTIK SISTEM KEAMANAN

Jebolnya sistem keamanan tentunya membawa dampak. Ada beberapa contoh akibat dari jebolnya sistem keamanan, antara lain:

- **Maret 2005.** Seorang mahasiswi dari UCSB dituduh melakukan kejahatan mengubah data-data nilai ujiannya (dan beberapa mahasiswa lainnya). Dia melakukan hal tersebut dengan mencuri identitas dua orang profesor. *Identity theft* memang merupakan sebuah masalah yang cukup pelik.

<http://www.dailynexus.com/news/2005/9237.html>

<http://it.slashdot.org/article.pl?sid=05/03/31/0339257&tid=146&tid=218>

BEBERAPA STATISTIK SISTEM KEAMANAN

Masalah keamanan yang berhubungan dengan Indonesia

Meskipun Internet di Indonesia masih dapat tergolong baru, sudah ada beberapa kasus yang berhubungan dengan keamanan di Indonesia. Dibawah ini akan didaftar beberapa contoh masalah atau topik tersebut.

- Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <[http:// www.2600.com](http://www.2600.com)> dan alldas.de
- Januari 2000. Beberapa situs web Indonesia diacak-acak oleh cracker yang menamakan dirinya “fabianclone” dan “naisenodni” (indonesian dibalik). Situs yang diserang termasuk Bursa Efek Jakarta, BCA, Indosatnet. Selain situs yang besar tersebut masih banyak situs lainnya yang tidak dilaporkan.

BEBERAPA STATISTIK SISTEM KEAMANAN

- **Akhir Januari 1999.** Domain yang digunakan untuk Timor Timur (.TP) diserang sehingga hilang. Domain untuk Timor Timur ini diletakkan pada sebuah server di Irlandia yang bernama *Connect-Ireland*. Pemerintah Indonesia yang disalahkan atau dianggap melakukan kegiatan *hacking* ini. Menurut keterangan yang diberikan oleh administrator Connect-Ireland, 18 serangan dilakukan secara serempak dari seluruh penjuru dunia. Akan tetapi berdasarkan pengamatan, domain Timor Timur tersebut dihack dan kemudian ditambahkan sub domain yang bernama “*need.tp*”. Berdasarkan pengamatan situasi, “*need.tp*” merupakan sebuah perkataan yang sedang dipopulerkan oleh “*Beavis and Butthead*” (sebuah acara TV di MTV). Dengan kata lain, crackers yang melakukan serangan tersebut kemungkinan penggemar (atau paling tidak, pernah nonton) acara *Beavis dan Butthead* itu. Jadi, kemungkinan dilakukan oleh seseorang dari Amerika Utara.

BEBERAPA STATISTIK SISTEM KEAMANAN

- Seorang cracker Indonesia (yang dikenal dengan nama hc) tertangkap di Singapura ketika mencoba menjebol sebuah perusahaan di Singapura.
- September dan Oktober 2000. Setelah berhasil membobol bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali. Perlu diketahui bahwa kedua bank ini memberikan layanan Internet banking.
- **September 2000.** Polisi mendapat banyak laporan dari luar negeri tentang adanya user Indonesia yang mencoba menipu user lain pada situs web yang menyediakan transaksi lelang (*auction*) seperti eBay.

BEBERAPA STATISTIK SISTEM KEAMANAN

- **24 Oktober 2000.** Dua warung Internet (Warnet) di Bandung digrebeg oleh Polisi (POLDA Jabar) dikarenakan mereka menggunakan account dialup curian dari ISP Centrin. Salah satu dari Warnet tersebut sedang online dengan menggunakan account curian tersebut.
- **April 2001.** Majalah Warta Ekonomi¹ melakukan polling secara online selama sebulan dan hasilnya menunjukkan bahwa dari 75 pengunjung, 37% mengatakan meragukan keamanan transaksi secara online, 38% meragukannya, dan 27% merasa aman.
- **16 April 2001.** Polda DIY meringkus seorang *carder*² Yogya. Tersangka diringkus di Bantul dengan barang bukti sebuah paket yang berisi lukisan (Rumah dan Orang Indian) berharga Rp 30 juta. Tersangka berstatus mahasiswa STIE Yogyakarta.

BEBERAPA STATISTIK SISTEM KEAMANAN

- **Juni 2001.** Seorang pengguna Internet Indonesia membuat beberapa situs yang mirip (persis sama) dengan situs klikbca.com, yang digunakan oleh BCA untuk memberikan layanan Internet banking. Situs yang dia buat menggunakan nama domain yang mirip dengan klikbca.com, yaitu kilkbca.com (perhatikan tulisan “kilk” yang sengaja salah ketik), wwwklikbca.com (tanpa titik antara kata “www” dan “klik”), clikbca.com, dan klickbca.com. Sang user mengaku bahwa dia mendapat memperoleh PIN dari beberapa nasabah BCA yang salah mengetikkan nama situs layanan Internet banking tersebut.

BEBERAPA STATISTIK SISTEM KEAMANAN

- **16 Oktober 2001.** Sistem BCA yang menggunakan VSAT terganggu selama beberapa jam. Akibatnya transaksi yang menggunakan fasilitas VSAT, seperti ATM, tidak dapat dilaksanakan. Tidak diketahui (tidak diberitakan) apa penyebabnya. Jumlah kerugian tidak diketahui.
- **Maret 2005.** Indonesia dan Malaysia berebut pulau Ambalat. Hacker Indonesia dan Malaysia berlomba-lomba untuk merusak situs-situs negara lainnya. Beberapa contoh halaman web yang dirusak di simpan di situs <http://www.zone-h.org>.

MENINGKATNYA KEJAHATAN KOMPUTER

Jumlah kejahatan komputer (*computer crime*), terutama yang berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain:

- Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat. Sebagai contoh saat ini mulai bermunculan aplikasi bisnis seperti *on-line banking*, *electronic commerce (e-commerce)*, *Electronic Data Interchange (EDI)*, dan masih banyak lainnya. Bahkan aplikasi *e-commerce* akan menjadi salah satu aplikasi pemacu di Indonesia (melalui “Telematika Indonesia” dan Nusantara). Demikian pula di berbagai penjuru dunia aplikasi ecommerce terlihat mulai meningkat.

MENINGKATNYA KEJAHATAN KOMPUTER

- Desentralisasi (dan *distributed*) server menyebabkan lebih banyak sistem yang harus ditangani. Hal ini membutuhkan lebih banyak operator dan administrator yang handal yang juga kemungkinan harus disebar di seluruh lokasi. Padahal mencari operator dan administrator yang handal adalah sangat sulit, apalagi jika harus disebar di berbagai tempat. Akibat dari hal ini adalah biasanya server-server di daerah (bukan pusat) tidak dikelola dengan baik sehingga lebih rentan terhadap serangan. Seorang cracker akan menyerang server di daerah lebih dahulu sebelum mencoba menyerang server pusat. Setelah itu dia akan menyusup melalui jalur belakang. (Biasanya dari daerah / cabang ke pusat ada routing dan tidak dibatasi dengan firewall.)

MENINGKATNYA KEJAHATAN KOMPUTER

- Transisi dari *single vendor* ke *multi-vendor* sehingga lebih banyak sistem atau perangkat yang harus dimengerti dan masalah *interoperability* antar vendor yang lebih sulit ditangani. Untuk memahami satu jenis perangkat dari satu vendor saja sudah susah, apalagi harus menangani berjenis-jenis perangkat. Bayangkan, untuk router saja sudah ada berbagai vendor; Cisco, Juniper Networks, Nortel, Linux-based router, BSD-based router, dan lain-lain. Belum lagi jenis sistem operasi (operating system) dari server, seperti Solaris (dengan berbagai versinya), Windows (NT, 2000, 2003), Linux (dengan berbagai distribusi), BSD (dengan berbagai variasinya mulai dari FreeBSD, OpenBSD, NetBSD). Jadi sebaiknya tidak menggunakan variasi yang terlalu banyak.

MENINGKATNYA KEJAHATAN KOMPUTER

- Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya (atau sistem milik orang lain). Jika dahulu akses ke komputer sangat sukar, maka sekarang komputer sudah merupakan barang yang mudah diperoleh dan banyak dipasang di sekolah serta rumah-rumah.



MENINGKATNYA KEJAHATAN KOMPUTER

- Mudahnya diperoleh software untuk menyerang komputer dan jaringan komputer. Banyak tempat di Internet yang menyediakan software yang langsung dapat diambil (*download*) dan langsung digunakan untuk menyerang dengan *Graphical User Interface* (GUI) yang mudah digunakan. Beberapa program, seperti SATAN, bahkan hanya membutuhkan sebuah web browser untuk menjalankannya. Sehingga, seseorang yang hanya dapat menggunakan web browser dapat menjalankan program penyerang (*attack*). Penyerang yang hanya bisa menjalankan program tanpa mengerti apa maksudnya disebut dengan istilah *script kiddie*.

MENINGKATNYA KEJAHATAN KOMPUTER

- Menggunakan satu jenis sistem juga tidak baik. Ini dikenal dengan istilah mono-culture, dimana hanya digunakan satu jenis sistem operasi saja atau satu vendor saja. Beberapa waktu yang lalu ada perdebatan mengenai mono-culture dan hetero-culture. Mana yang lebih baik? Kalau satu vendor saja, bila terkena masalah (virus misalnya yang hanya menyerang satu vendor itu saja), maka akan habis sistem kita. Akan tetapi jika terlalu bervariasi akan muncul masalah seperti diutarakan di atas.

MENINGKATNYA KEJAHATAN KOMPUTER

- Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat. Hukum yang berbasis ruang dan waktu akan mengalami kesulitan untuk mengatasi masalah yang justru terjadi pada sebuah sistem yang tidak memiliki ruang dan waktu. Barang bukti digital juga masih sulit diakui oleh pengadilan Indonesia sehingga menyulitkan dalam pengadilan. Akibatnya pelaku kejahatan cyber hanya dihukum secara ringan sehingga ada kecenderungan mereka melakukan hal itu kembali. (Hal ini akan dibahas lebih detail pada bagian hukum.)

MENINGKATNYA KEJAHATAN KOMPUTER

- 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). Lihat tabel di bawah untuk melihat peningkatan kompleksitas operating system Microsoft Windows. Seperti diungkapkan oleh Bruce Schneier dalam bukunya, “*complexity is the worst enemy of security*”.

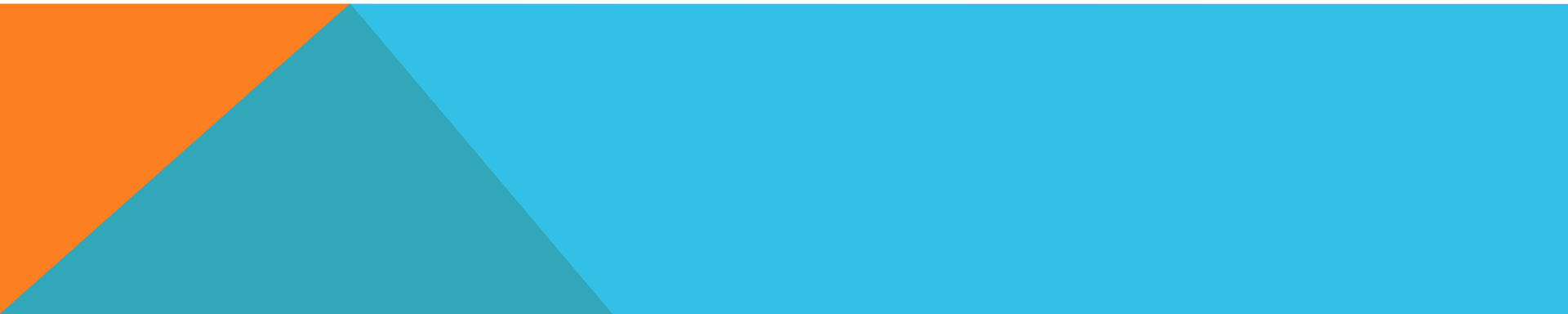
MENINGKATNYA KEJAHATAN KOMPUTER

TABLE 2. Trend meningkatnya kompleksitas software

Operating System Tahun	Jumlah baris code	(Lines of codes)
Windows 3.1	1992	3 juta
Windows NT	1992	4 juta
Windows 95	1995	15 juta
Windows NT 4.0	1996	16,5 juta
Windows 98	1998	18 juta
Windows 2000	2000	35 s/d 60 juta (perkiraan, tergantung dari sumber informasi)

MENINGKATNYA KEJAHATAN KOMPUTER

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.



KLASIFIKASI KEJAHATAN KOMPUTER

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*).

Menurut David Ilove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

- 1. Keamanan yang bersifat fisik (*physical security*):** termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Beberapa bekas penjahat komputer (*crackers*) mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan. Misalnya pernah diketemukan coretan password atau manual yang dibuang tanpa dihancurkan. Wiretapping atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.

KLASIFIKASI KEJAHATAN KOMPUTER

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*).

Menurut David Ilove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1. Pencurian komputer dan notebook juga merupakan kejahatan yang bersifat fisik. Menurut statistik, 15% perusahaan di Amerika pernah kehilangan notebook. Padahal biasanya notebook ini tidak dibackup (sehingga data-datanya hilang), dan juga seringkali digunakan untuk menyimpan data-data yang seharusnya sifatnya confidential (misalnya pertukaran email antar direktur yang menggunakan notebook tersebut).

KLASIFIKASI KEJAHATAN KOMPUTER

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*).

Menurut David Ilove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1. *Denial of service*, yaitu akibat yang ditimbulkan sehingga servis tidak dapat diterima oleh pemakai juga dapat dimasukkan ke dalam kelas ini. *Denial of service* dapat dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan). Beberapa waktu yang lalu ada lubang keamanan dari implementasi protokol TCP/IP yang dikenal dengan istilah *Syn Flood Attack*, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).

KLASIFIKASI KEJAHATAN KOMPUTER

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*).

Menurut David Ilove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1. Mematikan jalur listrik sehingga sistem menjadi tidak berfungsi juga merupakan serangan fisik. Masalah keamanan fisik ini mulai menarik perhatian ketika gedung World Trade Center yang dianggap sangat aman dihantam oleh pesawat terbang yang dibajak oleh teroris. Akibatnya banyak sistem yang tidak bisa hidup kembali karena tidak diamankan. Belum lagi hilangnya nyawa.

KLASIFIKASI KEJAHATAN KOMPUTER

2. Keamanan yang berhubungan dengan orang (personel): termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola). Ada sebuah teknik yang dikenal dengan istilah “*social engineering*” yang sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya kriminal ini berpura-pura sebagai pemakai yang lupa passwordnya dan minta agar diganti menjadi kata lain.

KLASIFIKASI KEJAHATAN KOMPUTER

3. **Keamanan dari data dan media serta teknik komunikasi** (*communications*). Yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang *virus* atau *trojan horse* sehingga dapat mengumpulkan informasi (seperti password) yang semestinya tidak berhak diakses. Bagian ini yang akan banyak kita bahas dalam buku ini.
4. **Keamanan dalam operasi:** termasuk kebijakan (*policy*) dan prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*). Seringkali perusahaan tidak memiliki dokumen kebijakan dan prosedur.

ASPEK / SERVIS DARI SECURITY

Garfinkel mengemukakan bahwa keamanan komputer (*computer security*) melingkupi empat aspek, yaitu

- privacy,
- integrity,
- authentication, dan
- availability.

Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu:


- access control dan
- non-repudiation.

ASPEK / SERVIS DARI SECURITY

Privacy / Confidentiality : Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator. Contoh *confidential information* adalah 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) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari confidentiality adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP).

ASPEK / SERVIS DARI SECURITY

Integrity: Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (*intercept*) di tengah jalan, diubah isinya (*altered, tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini.



ASPEK / SERVIS DARI SECURITY

Authentication : Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan digital signature. Watermarking juga dapat digunakan untuk menjaga “*intelektual property*”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat. Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

ASPEK / SERVIS DARI SECURITY

Availability ; Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan “*denial of service attack*” (DoS attack), dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirim 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 (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirim 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah.


ASPEK / SERVIS DARI SECURITY

Access Control : Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).



ASPEK / SERVIS DARI SECURITY

Non-repudiation : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan *digital signature*, *certificates*, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal.



Serangan Terhadap Keamanan Sistem INFORMASI

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 aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).

Serangan Terhadap Keamanan Sistem INFORMASI

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*):

- *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.