KEAMANAN SISTEM INFORMASI

Yuli Praptomo PHS
STMIK El Rahma – Yogyakarta

ABSTRACT

Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks. Security problem is one of important aspect from a information system. What a pity the problem of this security frequently less get attention from owners and organizer of information system. Oftentimes the problem of security reside in sequence, or even last sequence in lionized things list. If disturbing performansi of system, oftentimes security lessened or negated.

INTISARI

Keamanan Komputer sedang mencegah penyerang dari menuju keberhasilan sasaran hasil melalui atau sampai akses yang tidak sah atau penggunaan yang tidak sah tentang komputer dan jaringan. Keamanan masalah adalah salah satu dari aspek atau pengarah yang penting dari suatu sistem informasi. Sayang sekali permasalahan dalam keamanan ini sering lebih sedikit mendapatkan perhatian dari pemilik dan organisator dari sistem informasi. Seringkali permasalahan dalam keamanan berada atau terletak pada urutandibawah berbagai hal yang dianggap penting. Jika mengganggu performansi dari sistem, seringkali keamanan tidak atau kurang diperhitungkan.

Keyword : *information-based society, security hole, cheating, Asset*, *Vulnerabilities*, dan *Threats, managing threats, users, computer crime, on-line banking*, *electronic commerce (e-commerce)*, *Electronic Data Interchange.*

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali 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 menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. Tulisan ini diharapkan dapat memberikan gambaran dan informasi menyeluruh tentang keamanan sistem informasi dan dapat membantu para pemilik dan pengelola sistem informasi dalam mengamankan informasinya.

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.

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. 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.

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 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, Dissaster Recovery Center, dan seterusnya).

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 kegiatan yang dapat anda lakukan:

1. Hitung kerugian apabila sistem informasi anda tidak bekerja selama 1 jam, 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.)
2. 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.
3. 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.
4. 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.

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

TABLE 1. Kontribusi terhadap Risk

Nama komponen	Contoh dan keterangan lebih lanjut	
Assets (Aset)	♦ Hardware ♦ Software ♦ Dokumentasi ♦ Data	♦ Komunikasi ♦ Linkungan ♦ Manusia
Threats (ancaman)	♦ Pemakai (*users*) ♦ Teroris ♦ Kecelakaan (*accidents*) ♦ Crackers	♦ Penjahat kriminal ♦ Nasib (*acts of god*) ♦ Intel luar negeri (*foreign intelligence*)
Vulnerabilities (kelemahan)	♦ Software bugs ♦ Hardware bugs ♦ Radiasi (dari layar, transmisi) ♦ Tapping, crosstalk ♦ *Unauthorized users*	♦ Cetakan, *hardcopy* atau print out ♦ Keteledoran (*oversight*) ♦ Cracker via telepon ♦ Storage media

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

1. Usaha untuk mengurangi *threat*
2. Usaha untuk mengurangi *vulnerability*
3. Usaha untuk mengurangi impak (*impact*)
4. Mendeteksi kejadian yang tidak bersahabat (*hostile event*)
5. 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". Perusahan-perusahaan tersebut memilih untuk diam dan mencoba menangani sendiri masalah keamanannya tanpa publikasi.

1. 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.
2. 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.
3. 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.
4. 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).

5. 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 orangorang yang pernah mengirim email ke korban. Akibatnya file-file rahasia korban dapat terkirim tanpa diketahui oleh korban. Di sisi lain, orang yang dikirimi email ini dapat terinveksi 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 security hole ini dieksploit pada saat yang hampir bersamaan sehingga beban jaringan menjadi lebih berat.

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

1. 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.
2. 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport lokal (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan
3. 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.
4. 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. .
5. 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 .

Masalah keamanan yang berhubungan dengan Indonesia

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

1. **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.

2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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 medapat memperoleh PIN dari beberapa nasabah BCA yang salah mengetikkan nama situs layanan Internet banking tersebut.
8. **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:

1. 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.
2. 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.)

3. 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.
4. 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.
5. 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*.
6. 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.
7. 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 peningkatkan kompleksitas operating system Microsoft Windows. Seperti diungkapkan oleh Bruce Schneier dalam bukunya, "*complexity is the worst enemy of security*".

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 NT 4.0	1996	16,5 juta
Windows 95	1995	15 juta
Windows 98	1998	18 juta
Windows 2000	2000	35 s/d 60 juta (perkiraan, tergantung dari sumber informasi)

9. 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.

Alasan-alasan di atas membuat populernya bidang security saat ini.

Klasifikasi Kejahatan Komputer

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut David Icove 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. Pencurian komputer dan notebook juga merupakan kejahatan yang besifat 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). *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*). Mematikan jalur listrik sehingga sistem menjadi tidak berfungsi juga merupakan serangan fisik. Masalah keamanan fisik ini mulai menarik perhatikan 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.
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.
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.
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.

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).

Untuk mendapatkan kartu kredit, biasanya ditanyakan data-data pribadi. Jika saya mengetahui data-data pribadi anda, termasuk nama ibu anda, maka saya dapat melaporkan melalui telepon (dengan berpura-pura sebagai anda) bahwa kartu kredit anda hilang dan mohon penggunaannya diblokir. Institusi (bank) yang mengeluarkan kartu kredit anda akan percaya bahwa saya adalah anda dan akan menutup kartu kredit anda. Masih banyak lagi kekacauan yang dapat ditimbulkan bila data-data pribadi ini digunakan oleh orang yang tidak berhak.

Ada sebuah kasus dimana karyawan sebuah perusahaan dipecat dengan tidak hormat dari perusahaan yang bersangkutan karena kedapatan mengambil data-data gaji karyawan di perusahaan yang bersangkutan. Di perusahaan ini, daftar gaji termasuk informasi yang bersifat *confidential* / rahasia.

Dalam bidang kesehatan (*health care*) masalah privacy merupakan topik yang sangat serius di Amerika Serikat. *Health Insurance Portability and Accountability Act* (HIPPA), dikatakan akan mulai digunakan di tahun 2002, mengatakan bahwa rumah sakit, perusahaan asuransi, dan institusi lain yang berhubungan dengan kesehatan harus menjamin keamanan dan privacy dari data-data pasien. Data-data yang dikirim harus sesuai dengan format standar dan mekanisme pengamanan yang cukup baik. Partner bisnis dari institusi yang bersangkutan juga harus menjamin hal tersebut. Suatu hal yang cukup sulit dipenuhi. Pelanggaran akan *act* ini dapat didenda US$ 250.000 atau 10 tahun di penjara.

Serangan terhadap aspek privacy misalnya adalah usaha untuk melakukan penyadapan (dengan program *sniffer*). Usaha-usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi (dengan enkripsi dan dekripsi).

Ada beberapa masalah lain yang berhubungan dengan *confidentiality*. Apabila kita menduga seorang pemakai (sebut saja X) dari sebuah ISP (Z), maka dapatkah kita meminta ISP (Z) untuk membuka data-data tentang pemakai X tersebut? Di luar negeri, ISP Z akan menolak permintaan tersebut meskipun bukti-bukti bisa ditunjukkan bahwa pemakai X tersebut melakukan kejahatan. Biasanya ISP Z tersebut meminta kita untuk menunjukkan surat dari pihak penegak hukum (*subpoena*). Masalah privacy atau confidentiality ini sering digunakan sebagi pelindung oleh orang yang jahat/nakal.

Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin 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.

Salah satu contoh kasus trojan horse adalah distribusi paket program *TCP Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi trojan horse tersebut, maka ketika anda merakit (*compile*) program tersebut, dia akan mengirimkan eMail kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda. Informasi ini berasal dari CERT Advisory, "*CA-99-01 Trojan-TCP-Wrappers*" yang didistribusikan 21 Januari 1999. Contoh serangan lain adalah yang disebut "*man in the middle attack*" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

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 "*intelectual 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. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:

1. What you have (misalnya kartu ATM)
2. What you know (misalnya PIN atau password)
3. What you are (misalnya sidik jari, biometric)

Penggunaan teknologi *smart card*, saat ini kelihatannya dapat meningkatkan keamanan aspek ini. Secara umum, proteksi authentication dapat menggunakan *digital certificates*.

Authentication biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada server atau mesin. Pernahkan kita bertanya bahwa mesin ATM yang sedang kita gunakan memang benar-benar milik bank yang bersangkutan? Bagaimana jika ada orang nakal yang membuat mesin seperti ATM sebuah bank dan meletakkannya di tempat umum? Dia dapat menyadap data-data (informasi yang ada di magnetic strip) dan PIN dari orang yang tertipu. Memang membuat mesin ATM palsu tidak mudah. Tapi, bisa anda bayangkan betapa mudahnya membuat web site palsu yang menyamar sebagai web site sebuah bank yang memberikan layanan Internet Banking.

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 dikirimi 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 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 (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirimi 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah.

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).

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*, *certifiates*, 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. Hal ini akan dibahas lebih rinci pada bagian tersendiri.

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*):

1. *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “denial of service attack”.
2. *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
3. *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 pesanpesan yang merugikan pemilik web site.
4. *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesanpesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Mengapa sistem informasi berbasis Internet

Sistem informasi saat ini banyak yang mulai menggunakan basis Internet. Ini disebabkan Internet merupakan sebuah platform yang terbuka (*open platform*) sehingga menghilangkan ketergantungan perusahaan pada sebuah vendor tertentu seperti jika menggunakan sistem yang tertutup (*proprietary systems*). Open platform juga mempermudah interoperability antar vendor.

Selain alasan di atas, saat ini Internet merupakan media yang paling ekonomis untuk digunakan sebagai basis sistem informasi. Hubungan antar komputer di Internet dilakukan dengan menghubungkan diri ke link terdekat, sehingga hubungan fisik biasanya bersifat lokal. Perangkat lunak (*tools*) untuk menyediakan sistem informasi berbasis Internet (dalam bentuk server web, ftp, gopher), membuat informasi (HTML editor), dan untuk mengakses informasi (web browser) banyak tersedia. Perangkat lunak ini banyak yang tersedia secara murah dan bahkan gratis.

Statistik Internet

Jumlah komputer, server, atau lebih sering disebut *host* yang terdapat di Internet menaik dengan angka yang fantastis. Sejak tahun 1985 sampai dengan tahun 1997 tingkat perkembangannya (*growth rate*) jumlah host setiap tahunnya adalah 2,176. Jadi setiap tahun jumlah host meningkat lebih
dari dua kali. Pada saat naskah ini ditulis (akhir tahun 1999), growth rate sudah turun menjadi 1,5.

Data-data statistik tentang pertumbuhan jumlah host di Internet dapat diperoleh di “Matrix Maps Quarterly” yang diterbitkan oleh MIDS1.
Beberapa fakta menarik tentang Internet:

1. Jumlah host di Internet Desember 1969: 4
2. Jumlah host di Internet Agustus 1981: 213
3. Jumlah host di Internet Oktober 1989: 159.000
4. Jumlah host di Internet Januari 1992: 727.000

Statistik Electronic Commerce

Hampir mirip dengan statistik jumlah host di Internet, statistik penggunaan Internet untuk keperluan e-commerce juga meningkat dengan nilai yang menakjubkan. Berikut ini adalah beberapa data yang diperoleh dari International Data Corporation (IDC):

1. Perkiraan pembelian konsumer melalui Web di tahun 1999: US$ 31 billion (31 milyar dolar Amerika). Diperkirakan pada tahun 2003 angka ini menjadi US$177,7 billion.
2. Perkiraan pembelian bisnis melalui web di tahun 1999: US$80,4 billion (80,4 milyar dolar Amerika). Diperkirakan pada tahun 2003 angka ini menjadi US$1.1 trillion.

Di Indonesia, e-commerce merupakan sebuah tantangan yang perlu mendapat perhatian lebih serius. Ada beberapa hambatan dan juga peluang di dalam bidang ini.

Keamanan Sistem Internet

Untuk melihat keamanan sistem Internet perlu diketahui cara kerja sistem Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa sistem (router, gateway, hosts, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan. Kelemahan sebuat sistem terletak kepada komponen yang paling lemah.

Asal usul Internet kurang memperhatikan masalah keamanan. Ini mungkin dikarenakan unsur kental dari perguruan tinggi dan lembaga penelitian yang membangun Internet. Sebagai contoh, IP versi 4 yang digunakan di Internet banyak memiliki kelemahan. Hal ini dicoba diperbaiki dengan IP Secure dan IP versi 6.

Hackers, Crackers, dan Etika

Hackers are like kids putting a 10 pence piece on a railway line to see if the train can bend it, not realising that they risk de-railing the whole train (Mike Jones: London interview).

Untuk mempelajari masalah keamanan, ada baiknya juga mempelajari aspek dari pelaku yang terlibat dalam masalah keamanan ini, yaitu para hackers and crackers. Buku ini tidak bermaksud untuk membahas secara terperinci masalah non-teknis (misalnya sosial) dari hackers akan tetapi sekedar memberikan ulasan singkat.

Hackers vs crackers

HACKER. noun.

1. A person who enjoys learning the details of computer systems and how to stretch their capabilities - as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
2. One who programs enthusiastically or who enjoys programming rather than theorizing about programming. (Guy L. Steele, et al., *The Hacker’s Dictionary*)

hacker /n./
[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
3. A person capable of appre ciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker.

Sementara itu menurut Concise Oxfor English Dictionary
hacker /n.

1. *A person who or thing that hacks or cuts roughly.*
2. *A person whose uses computers for a hobby, esp. to gain unauthorized access to data.*

Istilah hackers sendiri masih belum baku karena bagi sebagian orang hackers mempunyai konotasi positif, sedangkan bagi sebagian lain memiliki konotasi negatif. Bagi kelompok yang pertama (*old school*), untuk pelaku yang jahat biasanya disebut *crackers*. Batas antara hacker dan cracker sangat tipis. Batasan ini ditentukan oleh etika. moral, dan integritas dari pelaku sendiri. Untuk selanjutnya dalam buku ini kami akan menggunakan kata hacker sebagai generalisir dari hacker dan cracker, kecuali bila diindikasikan secara eksplisit.

Paul Taylor dalam disertasi PhDnya mengungkapkan adanya tiga kelompok, yaitu *Computer Underground* (CU), *Computer Security Industry* (CSI), dan kelompok akademis. Perbedaan antar kelompok ini kadangkadang tidak tegas.

Untuk sistem yang berdomisili di Indonesia secara fisik (*physical*) maupun lojik (*logical*) ancaman keamanan dapat datang dari berbagai pihak.

Berdasarkan sumbernya, acaman dapat dikategorikan yang berasal dari luar negeri dan yang berasal dari dalam negeri. Acaman yang berasal dari luar negeri contohnya adalah hackers Portugal yang mengobrak-abrik beberapa web site milik pemerintah Indonesia.

Berdasarkan motif dari para perusak, ada yang berbasis politik, eknomi, dan ada juga yang hanya ingin mencari ketenaran. Masalah politik nampaknya sering menjadi alasan untuk menyerang sebuah sistem (baik di dalam maupun di luar negeri).
Beberapa contoh dari serangan yang menggunakan alasan politik antara lain:

1. Serangan dari hackers Portugal yang mengubah isi beberapa web site milik pemerintah Indonesia dikarenakan hackers tersebut tidak setuju dengan apa yang dilakukan oleh pemerintah Indonesia di Timor Timur. Selain mengubah isi web site, mereka juga mencoba merusak sistem yang ada dengan menghapus seluruh disk (jika bisa).
2. Serangan dari hackers Cina dan Taiwan terhadap beberapa web site Indonesia atas kerusuhan di Jakarta (Mei 1998) yang menyebabkan etnis Cina di Indonesia mendapat perlakukan yang tidak adil. Hackers ini mengubah beberapa web site Indonesia untuk menyatakan ketidaksukaan mereka atas apa yang telah terjadi.
3. Beberapa hackers di Amerika menyatakan akan merusak sistem milik pemerintah Iraq ketika terjeadi ketegangan politik antara Amerika dan Irak.

Interpretasi Etika Komputasi

Salah satu hal yang membedakan antara crackers dan hackers, atau antara Computer Underground dan Computer Security Industry adalah masalah etika. Keduanya memiliki basis etika yang berbeda atau mungkin memiliki interpretasi yang berbeda terhadap suatu topik yang berhubungan dengan masalah computing. Kembali, Paul Taylor melihat hal ini yang menjadi basis pembeda keduanya. Selain masalah kelompok, kelihatannya umur juga membedakan pandangan (interpretasi) terhadap suatu topik. Salah satu contoh, Computer Security Industry beranggapan bahwa Computer Underground masih belum memahami bahwa "*computing*" tidak sekedar permainan dan mereka (maksudnya CU) harus melepaskan diri dari "*playpen* (boks tempat bayi bermain)".

Perbedaan pendapat ini dapat muncul di berbagai topik. Sebagai contoh, bagaimana pendapat anda tentang memperkerjakan seorang hacker sebagai kepala keamanan sistem informasi anda? Ada yang berpendapat bahwa hal ini sama dengan memperkerjakan penjarah (gali, preman) sebagai kepala keamanan setempat. Jika analogi ini disepakati, maka akibat negatif yang ditimbulkan dapat dimengerti. Akan tetapi para computer underground berpendapat bahwa analogi tersebut kurang tepat. Para computer underground berpendapat bahwa hacking lebih mengarah ke kualitas intelektual dan jiwa pionir. Kalau dianalogikan, mungkin lebih ke arah permainan catur dan masa "*wild west*" (di Amerika jaman dahulu). Pembahasan yang lebih detail tentang hal ini dapat dibaca dalam disertasi dari Paul Taylor.

Perbedaan pendapat juga terjadi dalam masalah "*probing*", yaitu mencari tahu kelemahan sebuah sistem. Computer security industry beranggapan bahwa probing merupakan kegiatan yang tidak etis. Sementara para computer underground menganggap bahwa mereka membantu dengan menunjukkan adanya kelemahan dalam sebuah sistem (meskipun sistem tersebut bukan dalam pengelolaannya). Kalau dianalogikan ke dalam kehidupan sehari-hari (jika anda setuju dengan analoginya), bagaimana pendapat anda terhadap seseorang (yang tidak diminta) yang mencoba-coba membuka-buka pintu atau jendela rumah anda dengan alasan untuk menguji keamanan rumah anda.

Hackers dan crackers Indonesia

Apakah ada hackers dan crackers Indonesia? Tentunya ada. Kedua "school of thought" (madzhab) hackers ada di Indonesia. Kelompok yang menganut "old school" dimana hacking tidak dikaitkan dengan kejahatan elektronik umumnya bergabung di berbagai mailing list dan kelompok baik secara terbuka maupun tertutup. Ada beberapa mailing list dimana para hackers bergabung, antara lain :

1. Mailing list pau-mikro. Mailing list ini mungkin termasuk yang tertua di Indonesia, dimulai sejak akhir tahun 1980-an oleh yang sedang bersekolah di luar negeri (dimotori oleh staf PAU Mikroelektronika ITB dimana penulis merupakan salah satu motornya, yang kemudian malah menjadi minoritas di milis tersebut). Milis ini tadinya berkedudukan di jurusan elektro University of Manitoba, Canada (sehingga memiliki alamat pau-mikro@ee.umanitoba.ca) dan kemudian pindah menjadi paumikro@nusantara.net.
2. Hackerlink
3. Anti-Hackerlink, yang merupakan lawan dari Hackerlink
4. Kecoa Elektronik yang memiliki homepage sendiri di <http://k-elektronik.org>
5. Indosniffing dan masih banyak lainnya yang tidak mau dikenal atau kelopok yang hanya semusiman (kemudian hilang dan tentuny muncul yang baru lagi)

Selain tempat berkumpul hacker, ada juga tempat profesional untuk menjalankan security seperti di

1. IDCERT - Indonesia Computer Emergency Response Team http://www.cert.or.id
2. Mailing list diskusi@cert.or.id
3. Mailing list security@linux.or.id

Kesimpulan

Informasi merupakan komoditi yang sangat penting bagi sebuah organisasi baik comersial maupun individual. Oleh karena itu kemampuan untuk mengakses dan menyediakan informasi secara tepat dan akurat menjadi suatu hal yang sangat esensial.

Keamanan itu tidak dapat muncul demikian saja. Dia harus direncanakan. Jika tidak kita budgetkan di awal, kita akan dikagetkan dengan kebutuhan akan adanya perangkat pengamanan (firewall, Intrusion Detection System, anti virus, Dissaster Recovery Center, dan seterusnya).

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

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut David Icove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu: Keamanan yang bersifat fisik, Keamananyang berhubungan dengan orang, Keamanan dari data dan media serta teknik komunikasi, Keamanan dalam operasi.

Daftar Pustaka

1. Jogiyanto, 2002, Pengenalan Sistem Informasi, Andi Offset, Yogyakarta.
2. Kadir, A, 2002, Pengenalan Sistem Informasi, Andi Offset, Yogyakarta.
3. N-Top, Memantau Pengamanan Jaringan, Ftp://Ftp.ee.tbl.gov/libpcap.tar.2.
4. Raharjo, B, 1998, Keamanan Sistem Informasi Berbasis Internet, PT. Insan Mulia Indonesia, Bandung.

Biodata Penulis

Yuli Praptomo PHS, S.Kom adalah dosen tetap STMIK El Rahma Yogyakarta, lahir di Kulon Progo, 7 Juli 1972. Memperoleh gelar Sarjana Komputer, jurusan Teknik Informatika STMIK AKAKOM Yogyakarta pada tahun 1999, jabatan akademik terakhir Asisten Ahli, Sistem Informasi