URGENSI KEAMANAN PADA SISTEM INFORMASI

Article · October 2008

CITATIONS
5

READS
5,084

1 author:

Muhammad Irwan Padli Nasution
State Islamic University of Sumatera Utara, Medan Indonesia
29 PUBLICATIONS **38** CITATIONS

SEE PROFILE

URGENSI KEAMANAN PADA SISTEM INFORMASI

OLEH
Muhammad Irwan Padli Nasution

ABSTRACT

It's clear that taking the information and data by using the internet can facilitate the mankind to communicate with others around the world fastly. This development of technology had an effect on society in their socio-cultural and ethic. One of the biggest problem of using internet as a medium of information is the security of it's informations and data. This problem can take the priority when it's related to current needs. And it's very necessary to secure internet data and information from bugging, stealing, and damaging.

***Kata kunci**: data, informasi, komputer, internet, keamanan, organisasi*

1. Pendahuluan

Dalam sebuah organisasi dikenal ada 2(dua) sumber daya, yaitu sumber daya fisik dan konseptual berupa informasi. Sumber daya konseptual sangat penting dalam menunjang kelangsungan hidup suatu organisasi. Informasi yang akurat, *up-to-date,* dan dapat dipercaya sangat diperlukan dalam membantu pengambilan keputusan. Informasi akurat yang *real-time* dapat mempercepat pengambilan keputusan dan langkah pemecahan permasalahan yang dihadapi organisasi tertentu. Untuk mengolah data menjadi informasi, diperlukan teknologi informasi sebagai perangkat pengolah data dalam menjalankan aplikasi sistem informasi untuk menghasilkan suatu informasi yang diperlukan.

Komputer-komputer di era sekarang telah biasa terhubung satu dengan lainnya sehingga memungkinkan seorang pengguna dapat mengakses data atau informasi dari manapun dia berada dibelahan dunia ini tanpa perlu mengetahui lokasi fisik dari informasi tersebut. Untuk memungkinkan hal ini, diperlukan suatu perangkat keras maupun perangkat lunak yang harus memiliki konektivitas. Konektivitas merupakan isu penting di dalam kebebasan pengguna untuk menentukan solusi optimal akan berdampak timbulnya heterogenitas perangkat keras maupun perangkat lunak. Isu konektivitas heterogenitas ini dijawab dengan konsep *open system architecture* mengikuti aturan-aturan tertentu yang disepakati bersama untuk memberikan fasilitas komunikasi antar *system.* Satu hal yang muncul adalah semakin meluasnya penggunaan internet untuk keperluan interkoneksi antar komputer.

Peradaban dunia pada masa kini dicirikan dengan fenomena pertumbuhan internet dan globalisasi dihampir semua bidang kehidupan. Salah satu faktor pendorongnya adalah kemajuan teknologi yang berhasil membuahkan integrasi teknologi telekomunikasi, informasi dan multimedia. Ketika mereka masih berkembang sendiri - sendiri dampak yang dihasilkan belum sebesar sekarang, namun ketika telekomunikasi telah memperkaya teknologi informasi, keduanya menghasilkan jenis - jenis pelayanan baru yang sebelumnya tidak pernah terwujud. Pelayanan - pelayanan baru ini pada hakekatnya bertujuan memenuhi kebutuhan informasi yang disajikan dalam berbagai bentuk. Karena manusia menerbitkan dan menerima informasi menggunakan alat inderanya (mata, hidung, telinga, dan mulut), sehingga pelayanan inipun berupaya menyajikan informasi dalam kombinasi bentuk gambar, grafik, text, dan suara. Oleh karenanya penggunaan berbagai media sebagai data masukan atau informasi keluaran dari kombinasi alat telekomunikasi dan komputasi menjadi suatu keniscayaan.

Fenomena inilah yang kemudian disebut sebagai konvergensi teknologi telekomunikasi, informasi, dan multimedia. Kemajuan dan perkembangan teknologi, khususnya telekomunikasi, multimedia dan teknologi informasi (telematika) pada akhirnya merubah tatanan organisasi dan hubungan sosial kemasyarakatan. Hal ini tidak dapat dihindari, karena fleksibilitas dan kemampuan telematika untuk memasuki berbagai aspek kehidupan manusia. Bagi sebagian orang, telematika telah membuktikan perannya sebagai alat bantu yang memudahkan aktivitas kehidupan, sekaligus membantu meningkatkan produktivitas. Mereka yang sudah dapat menikmati manfaat telematika, terbukti mengalami peningkatan kekuatan ekonomi dan menjadi kelompok masyarakat yang relatif makmur, sebaliknya mereka yang belum memperoleh kesempatan pada umumnya berpenghasilan rendah dan bahkan di beberapa negara hidup dalam kemiskinan. Fenomena seperti ini makin menguatkan hipotesa *the winner takes all* yang kurang lebih menyiratkan makna bahwa yang kaya akan semakin kaya, sementara yang miskin tetap saja miskin. Internet sebagai perwujudan konvergensi telah menyebar ke seluruh penjuru dunia pada empat dekade terakhir ini, terutama di negara - negara yang memiliki kemampuan menyerap teknologi, dan oleh karenanya di negara-negara kaya kemudian terbentuk suatu kelompok yang disebut masyarakat informasi (Fukuyama, 2000). Transisi karakter ekonomi, sosial, dan budaya masyarakat cenderung berjalan lebih cepat ketika Internet melengkapi kemampuannya untuk memfasilitasi aktivitas bisnis dan perdagangan menjadi lebih efisien dan kompetitif.

2. Teknologi Informasi

Komputer generasi pertama dimulai pada tahun 1946. Komputer generasi ini adalah komputer elektronik yang menggunakan konsep *stored-program* (operasi komputer yang dikontrol oleh program dan disimpan di memori komputer). Program dibuat dengan bahasa mesin yang terdiri dari instruksi-instruksi angka 0 dan 1 di dalam urutan yang tertentu.

Penggunaan komputer akhirnya tidak hanya untuk keperluan penelitian dan bisnis, namun setiap orang ingin memilikinya, mempelajari dan mengembangkan kemampuannya melalui media komputer. Produsen mencermati fenomena ini, sehingga terciptalah komputer personal atau *Personal Computer* (PC). Sesuai dengan perkembangan teknologi selanjutnya, sehingga untuk keperluan bergerak *(mobile)* terciptalah komputer yang dapat dibawa kemana-mana. Misalnya

laptop, notebook dan palmtop. Komputer ini berukuran lebih kecil dari PC Desktop dan menggunakan tenaga baterai. Berat total hanya berkisar 1.5 kilogram.

Teknologi informasi merupakan suatu istilah dengan cakupan arti yang cukup luas. Definisi teknologi informasi itu sendiri masih sulit untuk dituangkan dalam suatu kalimat ringkas. Secara umum, teknologi informasi adalah suatu bidang yang menggeluti sekitar pemanfaatan teknologi untuk menghasilkan informasi, mengelola dan menyimpan informasi, mentransfer dari suatu bentuk ke bentuk yang lain, memindahkan dari suatu tempat ke tempat yang lain, atau bahkan mengolah informasi tersebut sehingga menjadi lebih mudah untuk digunakan oleh pemakainya.

Komponen-komponen yang diperlukan untuk membangun suatu teknologi informasi adalah teknologi sistem komputasi dan teknologi sistem komunikasi. Sistem komputasi berperan penting dalam mengolah sinyal-sinyal informasi tersebut sehingga dapat menghasilkan bentuk informasi yang paling sesuai dengan kebutuhan. Sistem komunikasi berperan dalam hal mentransfer sinyal-sinyal informasi dari suatu tempat ke tempat yang lain. Dengan semakin mengarahnya sistem komputasi menjadi *networked computing*, sehingga pembahasan komponen sistem komunikasi dalam teknologi informasi menjadi satu dengan komponen sistem komputasi.

Sistem komputer selalu terbangun dari dua komponen utama, yaitu perangkat keras *(hardware)* dan perangkat lunak *(software).* Keberadaan kedua komponen ini saling mendukung satu dengan yang lainnya. Perangkat keras tanpa perangkat lunak, ibarat ada sekumpulan benda terbuat dari plastik, kaca, dan besi yang tidak dapat mengerjakan sesuatu. Tanpa perangkat keras, perangkat lunak hanya merupakan kode-kode komputer yang tidak dapat menggerakkan perangkat keras.

- Perangkat Keras (*Hardware*), adalah kumpulan peralatan yang saling berhubungan satu sama lain. Peralatan ini berupa *CPU, disks, tapes, modem, cables,* dan lainnya. Perangkat keras ini dirancang khusus untuk mengikuti perintah/instruksi yang diberikan kepadanya. Dalam pengoperasiannya, sebuah komputer terdiri dari perangkat keras dan perangkat lunak. Keduanya saling berketergantungan. Pada dasarnya, perkembangan perangkat keras erat hubungannya dengan perkembangan arsitektur yang ada. Kini arsitektur yang ada dapat digolongkan menjadi dua, yakni arsitektur *CICS – Complex Instruction Set Computers (x86 Intel* prosesor) dan *RISC – Reduced Instruction Set Computers (Alpha, Power PC,* dan *Mips* prosesor).
- Perangkat Lunak *(Software),* adalah sekumpulan program yang dilengkapi dengan dokumentasi yang berhubungan secara langsung ke komputer, yang digunakan untuk menjalankan fungsi-fungsi yang diinginkan. Singkatnya, perangkat lunak adalah kumpulan instruksi-instruksi untuk sebuah komputer. Misalnya, perangkat lunak untuk manajemen data, inventorisasi, ataupun untuk pembuatan dokumentasi. Pengembangan perangkat lunak disini erat hubungan dengan perkembangan sistem operasi dan aplikasi yang dijalankan diatasnya. Berdasarkan data dari *Dataquest,* proyeksi sistem operasi yang akan mendominasi pasar tahun 2000 nantinya dapat digolongkan menjadi tiga, yakni *Microsoft Windows NT* sebesar 40 persen, *UNIX (*misalnya: *DIGITAL UNIX, HP-UX, IBM AIX, Sun SOLARIS,* dan lainnya*)* sebesar 40 persen, dan *Proprietary (*misalnya: *DIGITAL OpenVMS,*

IBM OS/400, SGI IRIX, dan lainnya) sebesar 20 persen, serta 90 persen menggunakan sistem gabungan dari ketiga katagori yang disebutkan tadi.

- Jasa/Layanan *(Services),* adalah sekumpulan aktivitas/pelayanan dalam rangka untuk memberikan nilai tambah dalam hubungan suatu proses bisnis (jual/beli). Baik itu berhubungan dengan produk yang dijual (perangkat keras dan/atau perangkat lunak) maupun pelayanan yang berupa konsultasi.

Oleh karena itu, perangkat keras merupakan subsistem dari sistem komputer. Seperti halnya dengan sistem komputer, perangkat keras terdiri dari beberapa komponen pendukung, yaitu alat masukan *(input device),* alat pemroses *(process device),* alat keluaran *(output device), memory,* alat penyimpanan *(storage device),* dan alat komunikasi *(communication device).*

Alat *input* atau masukan adalah alat yang berfungsi untuk menerima masukan berupa data, baik berupa numerik, karakter, string maupun gambar. Teknologi alat masukan berkembang sangat pesat, misalnya saja *keyboard, pointing device, scanner, sensor dan voice recognizer.*

Alat pemroses *(processing device)* adalah alat untuk mengeksekusi instruksi-instruksi program dan memproses data yang dimasukkan lewat alat masukan. Alat pemroses terdiri dari prosesor atau CPU dan memori utama *(main memory).*

CPU merupakan tempat pemrosesan instruksi-instruksi program. Pada komputer mikro, CPU disebut dengan *microprocessor.* CPU terdiri dari dua bagian utama, yaitu unit kendali atau *control unit* dan unit arithmatika dan logika atau *Arithmetic and Logical Unit* (ALU). Di samping dua bagian utama tersebut, CPU mempunyai beberapa simpanan yang berukuran kecil yang disebut dengan *register.*

Control Unit mengartikan instruksi-instruksi dari komputer, membawa data dari alat input ke main *memory,* dan mengambil data dari main *memory* untuk diolah. Bila ada perhitungan aritmatika atau perbandingan logika, maka control unit mengirim instruksi tersebut ke ALU. Hasil dari pengolahan data ini dibawa oleh control unit ke main *memory* untuk disimpan.

Alat *Output* bisa diartikan sebagai peralatan yang berfungsi untuk mengeluarkan hasil pemrosesan ataupun pengolahan data yang berasal dari CPU ke dalam suatu media yang dapat dibaca oleh manusia ataupun dapat digunakan untuk penyimpanan data hasil proses. *Output* yang dihasilkan dari pengolahan data dapat digolongkan ke dalam 3 (tiga) macam bentuk, yaitu:

a. Tulisan (huruf, kata, angka, karakter khusus, dan simbol-simbol lain).
b. Image (bentuk grafik atau gambar).
c. Suara (bentuk musik atau rekaman suara).

Kebutuhan akan media penyimpanan atau *storage device* saat ini sangatlah diperlukan. Dalam hal ini media penyimpanan dapat dibedakan menjadi 2(dua) macam, yaitu *internal storage dan external storage. Internal storage* terdiri dari *Random Access Memory* (RAM) dan *Read Only Memory* (ROM) berada dalam CPU. Sedangkan e*xternal storage* atau *external memory* merupakan suatu media atau sarana yang terletak di luar CPU yang dapat digunakan komputer untuk menyimpan data ataupun program. Media simpanan luar yang sifatnya pengaksesan secara langsung

telah dibutuhkan sejak komputer generasi pertama digunakan. Data yang tersimpan di dalam *external memory* bersifat tetap, artinya data tidak akan hilang walaupun tidak ada listrik yang mengalirinya.

Media yang digunakan umumnya merupakan media *magnetic* yang berfungsi sebagai tempat penyimpanan data dan informasi. Saat ini telah banyak beredar jenis *External Memory,* antara lain *floopy* disk, *harddisk,* USB *flash disk* , CD *ROM/*RW, dan lainnya.

Kecenderungan perkembangan komputer lebih terlihat kepada hal berikut:

- Ukuran fisik mengecil dengan kemampuan yang lebih besar
- Harga terjangkau (murah)
- Kemampuan penyimpanan data berkapasitas tinggi
- Transfer pengiriman data yang lebih cepat dengan adanya jaringan

3. Konsep Dasar Informasi

Informasi ibarat darah yang mengalir di dalam tubuh suatu organisasi, sehingga informasi ini sangat penting di dalam suatu organisasi. Suatu sistem yang kurang mendapatkan informasi akan menjadi luruh, kerdil dan akhirnya berakhir. Robert N. Anthony dan John Dearden menyebut keadaan dari sistem dalam hubungannya dengan keberaniannya dengan istilah entropy. Informasi yang berguna bagi sistem akan menghindari proses entropy yang disebut dengan *negative entropy* atau *negentropy.*[1]

Apakah sebenarnya informasi itu, sehingga sangat penting artinya bagi suatu sistem? Informasi (*information*) dapat didefinisikan sebagai berikut :

"Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya".

Sumber dari informasi adalah data. Data merupakan bentuk jamak dari bentuk tunggal datum atau item-item. Data adalah kenyataan-kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Kejadian-kejadian (*event*) adalah sesuatu yang terjadi pada saat yang tertentu. Di dalam dunia bisnis, kejadian-kejadian nyata yang sering terjadi adalah perubahan dari suatu nilai yang disebut dengan transaksi. Misalnya penjualan adalah transaksi perubahan nilai barang menjadi nilai uang atau nilai piutang dagang. Kesatuan nyata (*fact* dan *entity*) adalah berupa suatu obyek nyata seperti tempat, benda dan orang yang betul-betul ada dan terjadi. Informasi merupakan hal yang sangat penting bagi manajemen di dalam pengambilan keputusan. Pertanyaannya adalah darimana informasi tersebut bisa didapatkan? Informasi dapat diperoleh dari sistem informasi (*information systems*) atau disebut juga dengan *processing system* atau

[1]Robert N. Anthony, John Dearden, *Management Control System* (Edisi Keempat; Illinois: Richard D. Irwin), hal.125-126

information processing systems atau *information-generating systems*. Sistem informasi didefinisikan oleh Robert A.Leitch dan K.Roscoe Davis sebagai berikut:

> *Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan.*[2]

Menurut Gelinas, Oram, dan Wiggins (1990):

> *Sistem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis komputer dan manual yang dibuat untuk menghimpun, menyimpan, dan mengelola data serta menyediakan informasi keluaran kepada pemakai.*

Dari berbagai definisi tersebut, dapat disimpulkan bahwa sistem informasi mencakup sejumlah komponen (manusia, komputer, teknologi informasi, dan prosedur kerja), ada sesuatu yang diproses (data menjadi informasi), dan dimaksudkan untuk mencapai suatu sasaran atau tujuan.

Adanya perbedaan mutu informasi disebabkan oleh penyimpangan atau kesalahan. Pada umumnya kesalahan informasi merupakan masalah yang lebih sulit diatasi karena tidak mudah menyesuaikannya dibandingkan jika hanya terjadi penyimpangan informasi. Menurut Gordon B. Davis, kesalahan informasi antara lain dapat disebabkan oleh hal-hal sebagai berikut :

a. Metode pengumpulan dan pengukuran data yang tidak tepat
b. Tidak dapat mengikuti prosedur pengolahan yang benar
c. Hilang/ tidak terolahnya sebagian data
d. Pemeriksaan/pencatatan data yang salah
e. Dokumen induk yang salah
f. Kesalahan dalam prosedur pengolahan (misal: kesalahan program aplikasi komputer yang digunakan)
g. Kesalahan yang dilakukan secara sengaja

Penyebab kesalahan tersebut dapat diatasi dengan cara-cara sebagai berikut:

a. Kontrol sistem untuk menemukan kesalahan
b. Pemeriksaan internal dan eksternal
c. Penambahan batas ketelitian data
d. Instruksi dari pemakai yang terprogram secara baik dan dapat menilai adanya kesalahan-kesalahan yang mungkin terjadi.

[2]Robert A.Leitch /K.Roscoe Davis, *Accounting Information System*, (New Jersey Prentice-Hall, 1983), hal 6.

4. Bentuk Kejahatan Komputer

Celah atau lubang keamanan selain dapat ditemukan sebagai suatu akibat kompleksnya suatu sistem, dan dapat juga dibuat atau ditembus oleh para *criminal* atau *cracker* dengan keahlian yang dimilikinya. Para *criminal* selain mempunyai keahlian membongkar sistem keamanan juga dapat memperoleh informasi mengenai kelemahan sistem operasi dari internet sehingga memudahkan pekerjaan mereka.

National Institute of Standard and Technology (NIST) adalah sebuah divisi di bagian *United States Department of Commerce*, mengumpulkan beberapa kategori umum dari bentuk serangan terhadap komputer yaitu:[3]

a. Remote Penetration
b. Local Penetration
c. Remote Denial of Service (RDoS)
d. Local Denial of Service
e. Network Scanners
f. Vulnerability Scanners
g. Password Crackers.
h. Sniffers

Penjelasan untuk masing-masing kategori umum tersebut adalah sebagai berikut:

Remote Penetration: adalah sebuah program berbasis internet yang berkemapuan untuk masuk mengendalikan suatu komputer dengan cara tidak sah.

Local Penetration: adalah program-program yang berkemampuan untuk mengakses dengan tidak sah suatu komputer ketika programnya tersebut berjalan.

Remote Denial of Service: adalah sebuah program yang berjalan pada internet atau sebuah jaringan, dapat men-*shutdown* suatu komputer yang lain atau mematikan suatu layanan-layanan (*services*) yang disediakan oleh komputer tersebut

Local Denial of Service: adalah program-program yang dapat men-*shutdown* suatu komputer ketika suatu program lain berjalan. Sebuah penyerangan *Local Denial of Service* juga dapat mengakibatkan terputusnya koneksi sambungan sistem komputer secara fisik.

Network Scanners: adalah program-program yang mampu membuat pemetaan dari sebuah jaringan sehingga komputer-komputer tersebut mudah diserang dan tersedia untuk di eksploitasi.

Vulnerability Scanners: adalah program-program yang menggunakan internet untuk mencari komputer-komputer lain yang mudah untuk diserang dan ini adalah merupakan tipe-tipe dari bentuk penyerangan.

Password Crackers: adalah program-program yang mampu menemukan dengan mudah atau menerka suatu *password* walaupun file passwordnya telah dienkripsi.

[3]Joseph F. Gustin., "*Cyber Terrorism : A Guide for Facility Managers*", (The Fairmont Press., 2004), hal 26.

Sniffers 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 c*racker*, program sniffer dapat digunakan untuk menyadap password (jika dikirimkan dalam bentuk *clear text*).

Menurut Budi Rahardjo, jumlah kejahatan komputer (*computer crime*), terutama yang berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa alasan berikut:[4]

a. Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat. Sebagai contoh saat ini mulai bermunculan aplikasi bisnis seperti *on-line banking*, *electronic commerce (e-commerce)*, *Electronic Data Interchange* (EDI), dan masih banyak lainnya. Bahkan aplikasi *e-commerce* akan menjadi salah satu aplikasi pemacu di Indonesia (melalui "Telematika Indonesia" dan Nusantara-21). Demikian pula di berbagai penjuru dunia aplikasi ecommerce terlihat mulai meningkat.
b. Desentralisasi dan *distributed* server menyebabkan lebih banyak sistem yang harus ditangani. Hal ini membutuhkan lebih banyak operator dan administrator yang handal dan juga kemungkinan harus disebar ke 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.)
c. 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.
d. 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 digunakan di sekolah serta rumah-rumah.

[4]Budi Raharjo , "*Keamanan Sistem Informasi Berbasis Internet", (* PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta), 2005

e. 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*.
f. 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 di Indonesia sehingga menyulitkan dalam pengadilan. Akibatnya pelaku kejahatan *cyber* hanya dihukum secara ringan sehingga ada kecenderungan mereka akan melakukan hal itu kembali.
g. Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code*) yang digunakan sehingga semakin besar probabilitas terjadinya lubang keamanan (yang disebabkan kesalahan pemrograman, bugs).
h. 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 lokasi dimanapun menjadi lebih besar.

Politisi senior dari Partai Kebangkitan Bangsa AS, Hikam mengatakan:

> "p*erkembangan teknologi saat ini memang sangat pesat maka dari itu cyber crime juga bisa dipakai untuk tindakan terorisme*".

Keamanan itu tidak dapat muncul dengan sendirinya. Akan tetapi harus direncanakan. Misalnya, jika ingin membangun sebuah rumah, maka pintu rumah tersebut harus dilengkapi dengan kunci pintu. Jika terlupa memasukkan kunci pintu pada budget perencanaan pembangunan rumah, maka nantinya akan dikagetkan bahwa ternyata harus dikeluarkan 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 300 kamar dan lupa membudgetkan kunci pintu. Dampaknya sangat besar. Demikian pula di sisi pengamanan sebuah sistem informasi. Jika tidak dibudgetkan di awal, maka akan dikagetkan dengan kebutuhan akan adanya kebutuhan untuk perangkat pengamanan (*firewall, Intrusion Detection System, anti virus, Dissaster Recovery Center*, dan seterusnya). Meskipun sering terlihat bahwa besaran tersebut tidak dapat langsung diukur dengan uang (*intangible*). Akan tetapi keamanan sebuah sistem informasi sebetulnya dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible*). Dengan adanya ukuran yang jelas, mudah-mudahan pihak manajemen dapat mengerti akan pentingnya investasi di bidang keamanan informasi.

5. Keamanan Sistem Informasi

Teori informasi menekankan bahwa agar benar-benar mampu memberikan dukungannya kepada proses pengambilan keputusan manajerial dan agar aplikasinya tepat dan akurat, informasi yang dibutuhkan oleh suatu organisasi harus memenuhi persyaratan kelengkapan, kemutakhiran, kehandalan, terolah dengan baik, tersimpan dengan rapi dan mudah ditelusuri pada tempat penyimpanannya. Persyaratan-persyaratan tersebut hanya mungkin terpenuhi apabila data yang merupakan bahan baku untuk informasi, digali dari sumber-sumber yang tepat dan benar, dan dengan mutu yang tinggi. Teori ini perlu mendapat penekanan karena, seperti dimaklumi, data tidak mempunyai nilai intrinsik dalam proses pengambilan keputusan. Oleh karena itu, data yang dikumpulkan dari berbagai sumber, memerlukan pengolahan lebih lanjut agar sifatnya berubah menjadi informasi yang memiliki nilai sebagai alat pendukung proses pengambilan keputusan.

Menciptakan informasi tidak terlepas dari identifikasi dan penggalian sumber-sumber yang tepat dan benar. Sumber-sumber informasi yang dapat dan layak digali sangat bervariasi dari satu organisasi ke organisasi lain karena sangat tergantung pada proses pengambilan keputusan apa yang akan didukungnya dan untuk kepentingan apa infomasi tersebut akan dipergunakan. Setiap orang yang pernah berkecimpung dalam kegiatan pengolahan informasi pasti mengetahui bahwa sumber-sumber tersebut dapat berada di dalam suatu organisasi seperti berbagai satuan kerja yang terdapat di dalamnya akan tetapi dapat pula berada di luar organisasi yang bersangkutan. Instrumen untuk memperolehnyapun dapat beraneka ragam.

Masalah keamanan sistem informasi menempati kedudukan yang sangat penting, akan tetapi perhatian para pemilik dan pengelola sistem informasi relatif masih kurang, bahkan menempati kedudukan kedua atau berikutnya dalam daftar-daftar berbagai hal yang dianggap penting dalam pengelolaan sistem informasi berbasis internet. Ada beberapa hal yang harus dilindungi dalam sebuah sistem jaringan informasi global berbasis internet (*cyberspace*), yaitu :

a. Isi/substansi data dan/atau informasi yang merupakan *input* dan *output* dari penyelenggara sistem informasi dan disampaikan kepada *public* atau disebut juga dengan *content*. Dalam hal penyimpanan data dan /atau informasi tersebut akan disimpan dalam bentuk *databases* dan dikomunikasikan dalam bentuk *data messages*;
b. Sistem pengolahan informasi (*computing and/or information system*) merupakan jaringan sistem informasi organisasional yang efisien, efektif dan legal. Dalam hal suatu sistem informasi merupakan perwujudan penerapan perkembangan teknologi informasi ke dalam suatu bentuk organisasional /organisasi perusahaan (bisnis);
c. Sistem komunikasi (*communication*) merupakan perwujudan dari sistem keterhubungan (*interconnection*) dan sistem pengoperasian global (*inter operational*) antar sistem informasi /jaringan komputer (*computer network*) maupun penyelenggaraan jasa dan/atau jaringan telekomunikasi; dan
d. Masyarakat (*community*) yang merupakan perangkat intelektual (*brainware*), baik dalam kedudukannya sebagai pelaku usaha, professional penunjang maupun pengguna.

Menjaga keempat aspek tersebut merupakan bagian dari *policy* keamanan sistem informasi. Keamanan sistem informasi berbasis internet merupakan suatu keharusan yang harus diperhatikan karena jaringan komputer internet sifatnya *public* dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar informasi yang berharga itu dapat terlindungi secara efektif. Untuk mencapai semua itu, jaringan komputer harus dianalisis sehingga diketahui apa yang harus dan untuk apa diamankan, serta seberapa besar nilainya.

Keamanan komputer (*computer security*) melingkupi 4 (empat) aspek, yaitu *privacy, integrity, authentication* dan *availability*. Selain keempat aspek itu masih ada 2 (dua) aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation*. Aspek utama dari *privacy* atau *confidentially* adalah usaha untuk menghindarkan penggunaan informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data yang sifatnya *private*, sedangkan *confidentially* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Sebagai contoh misalnya yang berhubungan dengan *privacy* adalah *email* seseorang pemakai (*user*) tidak boleh dibaca oleh *administrator*, sedangkan contoh *confidentially information* adalah data yang sifatnya pribadi dan merupakan data yang diproteksi penggunaanya dan penyebarannya. Serangan terhadap aspek *privacy* ini misalnya adalah usaha untuk melakukan penyadapan (*sniffing*). Usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentially* adalah dengan menggunakan teknologi kriptografi (*enkripsi* dan *deskripsi data*).

Dalam lingkup *cyberlaw,* yang termasuk *privacy* ada 4 (empat) kategori, yaitu :

a. *Protection from intrusion;*
b. *Protection from the public disclosure of embarrassing private facts;*
c. *Protection from publicity that places the individual in a false light; and*
d. *Protection from the use of a person's name or likeness.*

Teknologi kriptografi menjelaskan bagaimana mengamankan data dengan menggunakan enkripsi. Tujuan utama dari solusi ini adalah mencegah terjadinya curi-dengar (*eavesdropping*) terhadap data yang dikirimkan maupun yang diterima. Jika seorang "*eavesdropper*" melakukan tindakan curi-dengar, ia akan memperoleh data yang ter-*enkripsi* saja sehingga tidak mencerminkan isi data yang sebenarnya.

Aspek *integrity* menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi tersebut. Aspek *authentication* berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi tersebut adalah betul-betul orang yang dimaksud. Masalah pertama membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan *digital signature*. *Watermarking* dapat juga digunakan untuk menjaga *intellectual 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. Secara umum proteksi *authentication* dapat menggunakan *digital certificates*.

Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. System 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)*, yaitu server dikirimi permintaan (biasanya palsu yang bertubi-tubi atau permintaan yang di luar perkiraan sehingga server tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirimi email bertubi-tubi (katakanlah ribuan email) dengan ukuran yang besar sehingga si pemilik email kesulitan untuk mengakses emailnya atau bahkan tidak dapat membuka emailnya. Serangan terhadap *availability* dalam bentuk *Denial of Service* (DoS attack) merupakan yang terpopuler pada saat ini.

Access control berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. Access *control* sering kali dilakukan dengan menggunakan kombinasi user-id dan *password*.. Aspek *non-repudiation* ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Contohnya jika seseorang mengirimkan email untuk memesan suatu barang, maka ia tidak akan dapat menyangkal bahwa benar dia telah mengirimkan email tersebut.

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

6. Kesimpulan

Data yang diolah menjadi suatu informasi merupakan bahan referensi penting di dalam pengambilan suatu keputusan. Pemanfaatan teknologi informasi untuk pengolahan data dan pertukaran data atau informasi sangat berkembang pesat. Data dan informasi dapat mengalir dengan sangat cepat dari suatu tempat ke tempat lain walaupun lokasinya berjauhan. Waktu, tempat dan wilayah tidak akan membatasi aliran data dan informasi ini. Misalnya pada saat mengirimkan data atau informasi melalui jaringan internet, kita selalu ingin agar data atau informasi yang dikirimkan tersebut sampai ke tujuan dengan selamat dan tidak akan mengalami campur tangan pihak lain. Oleh sebab itu semakin diperlukan suatu proteksi untuk melindungi data atau informasi tersebut dari pencurian, penyadapan maupun pengrusakan oleh berbagai pihak lain secara ilegal.

DAFTAR PUSTAKA

Davis, G.B. & Olson, M.H., "*Management Information system: Conceptual Foundations, Structure and Development"* (2nd edition). New York : McGraw-Hill., 1984.

Efraim Turban, Ephrain McLean, James Wetherbe, "*Information Technology For Management",* John Wiley & Sons Inc, 2001.

Gustin, Joseph F., "*Cyber Terrorism : A Guide for Facility Managers*", The Fairmont Press., 2004.

McLeod, Raymond Jr, "*Management Information Systems*", 8th Edition, Prentice Hall, Inc., 2001.

Raharjo, Budi , "*Keamanan Sistem Informasi Berbasis Internet",* PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta, 2005

http://www.theonion.com/content/node/28467, kutipan 26 Pebruari 2007.

http://chronicle.com/errors.dir/noauthorization.php3?page=/weekly/v47/i24/24a 04402.htm, kutipan 26 Pebruari 2007.

http://www.ipsentry.com/scr, kutipan 26 Pebruari 2007.

http://www.cyberspacelaw.org, kutipan 26 Pebruari 2007

http://www.dpr.go.id/artikel/artikel.php?aid=1076, kutipan 26 Pebruari 2007.