MENGAMANKAN TRANSAKSI DI INTERNET: SUATU TINJAUAN TERHADAP JUSTIFIKASI DAN METODE

Adi Cahyadi[1]

ABSTRACT

Securing internet transaction has become more crucial considering the rise of cyber crime. Although many business owners have become aware of this, the implementation of security technology especially in developing countries is still somewhat slow and this is not apart from the fact that securing electronic transaction is costly. Improper consulting practice has also resulted in an overspending of budget for security projects. This article tries to shed some light to its readers and business owners on the proper practice of evaluating a security investment, selecting an appropriate security solution as well as introducing major methods of securing an electronic transaction.

Keywords: *internet, transaction, justification, method*

ABSTRAK

Mengamankan transaksi di internet menjadi hal yang semakin penting, terlebih dengan meningkatnya tindak kriminalitas di dunia cyber. Walaupun banyak pengusaha menyadari hal itu, implementasi dan aplikasi teknologi pengamanan, khususnya di negara sedang berkembang, masih relatif lambat dan hal itu tidak terlepas dari kenyataan bahwa biaya mengamankan transaksi elektronik relatif mahal. Kendala itu diperburuk dengan adanya praktik yang tidak terpuji dari para konsultan yang cenderung merekomendasikan produk/teknologi yang sebenarnya tidak dibutuhkan perusahaan. Artikel ini mencoba memberikan sedikit gambaran kepada para pembaca dan para pemilik usaha e-business mengenai praktik yang benar dalam menilai kelayakan investasi di bidang keamanan data dan dalam memilih solusi dan produk keamanan yang tepat bagi usahanya. Juga memperkenalkan sejumlah metode utama yang banyak digunakan dalam mengamankan jaringan komputer serta transaksi elektronik.

Kata kunci: *internet, transaksi, justifikasi, metode*

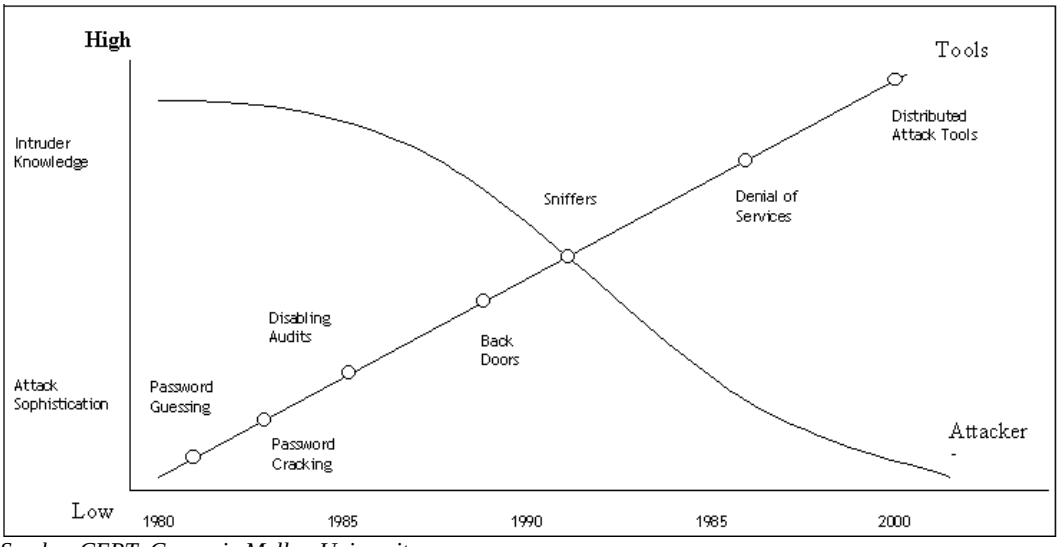
[1] **Staf Pengajar Universitas Trisakti & UBiNus, Jakarta**

PENDAHULUAN

Pentingnya Mengamankan Transaksi di Internet

Sejak digagasnya konsep bertransaksi lewat media internet, banyak pihak mempertanyakan keamanannya. Hal itu tidak terlepas dari sifat internet itu sendiri yang terbuka dan bebas diakses oleh pihak manapun. Kekhawatiran akan keamanan bertransaksi di internet semakin meningkat setelah banyak perusahaan mulai menggunakan internet untuk tujuan bisnis, terlebih setelah khawatiran tersebut terbukti dengan terjadinya berbagai kasus pembobolan *server*, pencurian data, dan penyerangan terhadap sejumlah situs yang mengkibatkan kerugian yang cukup signifikan.

Kegiatan pelanggaran hukum (*Cyber Crime*) semakin meningkat pada dasawarsa belakangan ini, akibat semakin mudahnya seorang pengguna internet memperoleh perangkat lunak yang diperlukan untuk melakukan penyerangan terhadap suatu situs. Kecenderungan itu terlihat pada hasil survei yang dilakukan oleh CERT (*Computer Emergency Response Team*), suatu tim yang dibentuk oleh Carnegie Mellon University untuk meneliti dan mendukung pemecahan masalah keamanan komputer yang timbul. Survei itu menemukan bahwa dilihat dari tingkat kecanggihan serangan dan tingkat keahlian penyerang, terjadi suatu kecenderungan yang kontras (berlawanan). Dari tahun 1980-an sampai awal 2000, tingkat kecanggihan penyerangan semakin meningkat namun sebaliknya, tingkat keahlian penyerang memperlihatkan kecenderungan menurun.



Sumber CERT, Carnegie Mellon University

Gambar 1 Grafik Tren Tingkat Kecanggihan Penyerangan dan Keahlian Penyerang

Terlihat dari grafik tersebut bahwa mendekati abad ke-21, tingkat kecanggihan serangan semakin meningkat mulai dari sekedar menebak *login password*, membobol *password*, sampai pada melakukan serangan terdistribusi terhadap suatu sasaran (situs). Selain tingkat kecanggihan serangan yang meningkat, frekuensi serangan pun semakin meningkat dan hal itu dikonfirmasi oleh hasil survei yang diadakan oleh Lembaga Penyidik Federal AS (*Federal Bureau of Investigation*) pada tahun 2000, yaitu 70% dari 643 responden yang diwawancara menyatakan pernah diserang atau menjadi korban pembobolan. Angka itu meningkat 42% dari tahun 1996.

Kecenderungan itu juga dikuatkan oleh hasil pendataan CERT yang menunjukkan adanya kenaikan jumlah laporan tindak kriminal yang menggunakan teknologi komputer. Dari 2.600 laporan pada tahun 1996 menjadi 10.000 laporan pada tahun 1999 dan bahkan melonjak menjadi 22.000 laporan pada tahun 2000, seperti yang terlihat pada Tabel 1 di bawah ini.

Tabel 1 Insiden dan Kelemahan Sistem Informasi yang Dilaporkan pada CERT

	1996	1997	1998	1999	2000
Insiden	2.573	2.134	3.734	9.859	21.756
Kelemahan	345	311	262	417	774

Sumber: CERT

Meningkatnya kecanggihan serangan, menurunnya level keahlian penyerang, serta meningkatnya frekuensi penyerangan mengindikasikan lahirnya suatu kelompok pelanggar hukum baru yang menggunakan aplikasi yang disediakan oleh seorang *programmer* ahli untuk melakukan suatu tindak kriminal. Dengan adanya kelompok baru itu, populasi pengguna internet yang berpotensi melakukan tindak kriminal (*cyber crime*) meningkat tajam. Hal itulah yang menjadikan transaksi di internet semakin rentan dan memerlukan pengamanan.

PEMBAHASAN

Hambatan Mengembangkan Sistem Keamanan Transaksi di Internet

Banyak pengusaha e-business memulai langkah pengamanan transaksi bisnisnya dengan menyewa konsultan untuk mengidentifikasikan kelemahan sistem informasi yang dimilikinya sekaligus memberikan masukan bagi pengusaha mengenai teknologi keamanan data yang harus dimilikinya. Ketergantungan pengusaha terhadap informasi dan masukkan konsultan menjadikan mereka rentan terhadap praktik penipuan dan para konsultan mengusulkan suatu sistem keamanan yang berlebihan untuk mengejar nilai kontrak yang maksimal. Mahalnya biaya konsultasi dan pengembangan sistem keamanan itulah yang menyebabkan banyak perusahaan menunda investasinya pada hal yang kritis ini.

Dilema di atas tidak perlu terjadi bila para pengusaha memahami pedoman utama dalam melakukan investasi di bidang keamanan data yang menyebutkan bahwa “justifikasi investasi di bidang keamanan data tergantung dari rasio antara nilai investasi yang diperlukan untuk mengamankan data pada suatu periode dan nilai kerugian potensial dari dicurinya/diubahnya/dirusaknya data oleh pihak yang tidak bertanggung-jawab sedangkan nilai

kerugian potensial itu sendiri merupakan hasil pengalian antara nilai kerugian per insiden dengan peluang terjadinya insiden dalam suatu periode". Cara pengukuran itu secara lebih jelas dapat dilihat pada formula sederhana berikut ini.

$$\text{Nilai Justifikasi} = \frac{\text{Nilai Investasi Keamanan Data pada Suatu Periode (NIKD)}}{\text{Nilai Kerugian Potensial pada suatu Periode (NKP)}}$$

$$\text{Nilai Kerugian Potensial} = \text{Nilai Kerugian per Insiden} \times \text{Peluang terjadinya insiden pada suatu periode}$$

Menggunakan rumus tersebut, seorang pengusaha dapat menentukan apakah suatu data atau aset layak untuk mendapatkan perlindungan tertentu atau tidak. Sebagai contoh, bila nilai justifikasi suatu investasi kurang dari 1 berari bahwa Nilai Kerugian Potensialnya lebih besar dari Nilai Investasinya sehingga investasi tersebut dapat dibenarkan. Sebaliknya, bila nilai justifikasinya lebih besar dari 1 berarti bahwa nilai investasi lebih besar dari nilai kerugian potensial maka investasi tersebut tidak dapat dibenarkan secara finansial.

Konsep Keamanan Bertransaksi di Internet

Keputusan atas metode dan teknologi keamanan yang tepat untuk mengamankan suatu transaksi selain dapat dilihat dari segi finansial, juga dapat dilihat dari definisi keamanan transaksi itu sendiri. Pada beberapa literatur disebutkan bahwa keamanan bertransaksi terjadi bila pengusaha dapat menjamin adanya hal berikut.

1. *Privacy/Confidentiality* (Kerahasiaan), yaitu kerahasiaan data pelanggan dan perusahaan dari pihak yang tidak berkepentingan.
2. *Authenticity* (Otentisitas), yaitu kepastian bahwa data atau informasi yang terlihat pada situs melalui *browser* atau yang dikirim melalui *e-mail* adalah benar informasi dari perusahaan atau orang yang menjadi lawan transaksi.
3. *Authorization* (Otorisasi) atau Akses, yaitu kepastian bahwa orang yang mengakses data, *server*, atau jaringan adalah benar orang yang berkepentingan atau diberikan kewenangan untuk berbuat demikian.
4. *Availability* (Ketersediaan), yaitu kepastian bahwa seorang pengguna yang berkepentingan (karyawan, konsumen, pemasok, atau rekanan) perusahaan dapat mengakses data atau jaringan perusahaan kapan pun diperlukan.
5. *Integrity* (Integritas), yaitu kepastian bahwa data yang dikirim atau disimpan belum diubah atau dimanipulasi.

Kelima kualitas itu menentukan amannya suatu transaksi di internet sehingga bila ingin melakukan investasi dalam mengamankan transaksi dengan pelanggan di internet, kelima faktor itu perlu dipenuhi.

Metode Pendukung Keamanan Bertransaksi di Internet

Berdasarkan nilai atau faktor yang digunakan dalam mengukur keamanan bertransaksi di

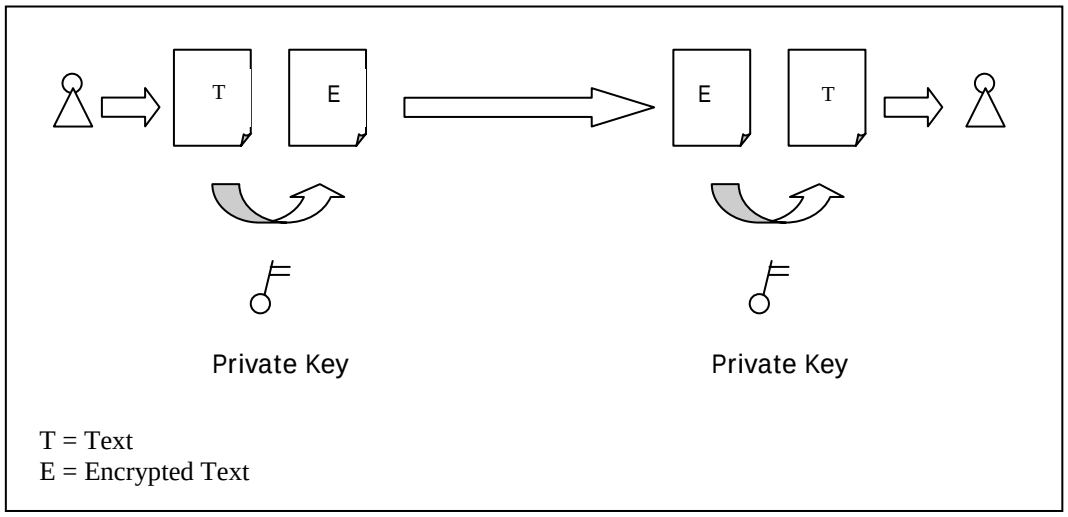
internet, alat atau metode pengamanan (*security tools*) yang perlu diperhatikan oleh seorang pengusaha atau lembaga yang ingin melakukan transaksi melalui internet dibagi menjadi lima kategori berikut.

1. Metode yang mendukung kerahasiaan data.
2. Metode yang mendukung otentikasi pengguna.
3. Metode yang mendukung keamanan akses ke jaringan computer.
4. Metode yang mendukung ketersediaan layanan (*availability*).
5. Metode yang mendukung keutuhan data (*intergrity*).

1. Metode yang Mendukung Kerahasiaan Data

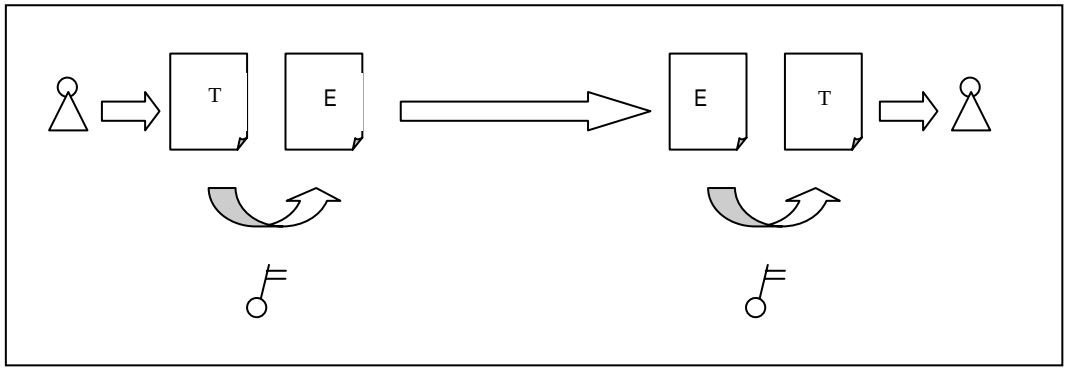
Kerahasiaan data dapat didukung oleh teknologi enkripsi (*encryption technology*), yaitu suatu teknologi *software* yang menggunakan formula matematik untuk mengacak (*encrypt*) data yang akan dikirim. Teknologi itu juga memungkinkan data yang telah diacak untuk dikembalikan dalam bentuk semula (*decrypt*) oleh si penerima pesan. Teknologi enkripsi itu memiliki dua pendekatan sebagai berikut.

1. Pendekatan *Private Key Encryption*. Pada pendekatan itu, kunci yang sama dipakai untuk mengenkripsi (mengacak) dan mendekripsi (menyusun ulang) data seperti yang terlihat pada diagram di bawah ini.



Gambar 2 Bagan Cara Kerja *Private Key Encryption*

2. Pendekatan *Public Key Encryption*. Pada pendekatan itu, dua kunci yang berbeda dipakai untuk mengenkripsi (mengacak) dan mendekripsi(menyusun ulang) data. Kunci yang disebut *Public Key* dipakai untuk mengenkripsi data sedangkan kunci pembuka yang disebut sebagai *Private Key* dipakai untuk menyusun ulang data. Seperti yang terlihat pada diagram di bawah ini.



Gambar 3 Bagan Cara Kerja *Public Key Encryption*

Pendekatan kedua itu dinilai lebih aman karena kunci pembuka, yaitu *private key* tidak perlu didistribusikan. Pendistribusian yang diperlukan ialah kunci pengacaknya sehingga walaupun kunci tersebut dicuri oleh seorang *hacker*, ia belum dapat membuka kode yang hanya dapat disusun kembali oleh kunci *private* (*private key*). Metode kedua yang dilakukan untuk menjamin *Privacy* adalah melakukan pengamanan pada sisi *End User* dan *Server* (*End User and Server Security*). Pada metode *End-User Security*, para pemakai komputer perlu diberikan pengarahan bahkan perlu diinformasikan mengenai peraturan penggunaan fasilitas internet maupun fasilitas TI lainnya. Para pemakai komputer juga perlu dibimbing (*supervised*) untuk melakukan kegiatan bisnisnya sesuai dengan aturan main yang telah ditetapkan perusahaan, termasuk dalam penggunaan sistem informasi perusahaan. Terakhir, para pemakai komputer perlu pula diawasi dalam hal pemakaian dan penggunaan fasilitas TI perusahaan. Pada metode *Server Security*, *server* perlu dilindungi dengan cara berikut.

a. Membuat *Privacy Policy*, yaitu organisasi membuat dan mensosialisasikan peraturannya mengenai kerahasiaan data yang dipertukarkan dalam jaringan sistem informasinya berikut alokasi kewenangan mengakses data.
b. Membatasi akses ke *server* semua alat yang terhubung dengan *server* harus diamankan untuk menjamin tidak adanya akses yang tidak dibenarkan.
c. Mengamankan *e-mail* karena *e-mail* sering menjadi sumber masuknya virus dan program destruktif lainnya.

2. Metode yang Mendukung Otentikasi Pengguna (*Authentication*)

Tujuan utama otentikasi adalah menjamin bahwa pihak yang mengirim data adalah benar pihak yang merupakan lawan transaksi, seperti yang diklaim olehnya. Otentikasi dapat dilakukan melalui dua cara berikut.

1. Pembenaran terhadap jati diri seseorang.

Pembenaran terhadap jati diri seseorang dapat dilakukan melalui tiga hal sebagai berikut.

a. Dengan memberikan *password* atau *username* saat mengakses/*login* ke suatu *server* atau situs. Pendekatan itu disebut sebagai otentikasi menggunakan informasi yang hanya orang tersebut tahu (*authentication based on what you know*).
b. Dengan melakukan penginderaan (*scanning*) terhadap salah satu bagian anggota tubuh, seperti retina mata, wajah, sidik jari, suara, dan sebagainya. Metode itu disebut juga sebagai metode *Biometric Security* atau metode otentikasi dengan mengklarifikasikan diri berdasarkan anggota tubuh yang dimiliki (*authentication based on what you are*).
c. Dengan memberikan sesuatu yang hanya yang hanya dimiliki pribadi, seperti menggesek bagian strip magnetis kartu identitas. Metode otentikasi itu disebut juga otentikasi berdasarkan yang dimiliki (*authentication based on something you posses*).

2. Pembenaran menggunakan *Digital Signatures* dan *Digital Certificate*.

a. Tanda Tangan Digital (*Digital Signatures*)
Bila tanda tangan seseorang memperlihatkan keunikan identitas seseorang, tanda tangan digital memperlihatkan keaslian pengirim sebuah pesan elektronik. Cara kerja tanda tangan digital (*digital signature*) sebagai berikut.
   - Bila seorang pengirim hendak mengirim pesan. Pesan tersebut diproses menggunakan algoritma matematik sehingga menghasilkan sederet karakter yang mewakili keseluruhan dokumen. Proses itu disebut "*Hashing*". Sederet karakter hasil proses itulah yang disebut tanda tangan digital.
   - Tanda tangan digital itu dienkripsi (diacak) menggunakan kunci enkripsi.
   - Pada saat si penerima menerima pesan tersebut, pesan asli yang diterimanya diproses menggunakan algoritma yang sama dengan milik si pengirim untuk menghasilkan sederet karakter yang merupakan tanda tangan digital (*digital signature*).
   - Tanda tangan digital yang diterima B dari pengirim dibuka menggunakan kunci enkripsi sehingga menghasilkan set/deret karakter kedua.
   - Kedua set/deret karakter itu dibandingkan untuk melihat apakah pesan tersebut otentik atau tidak.

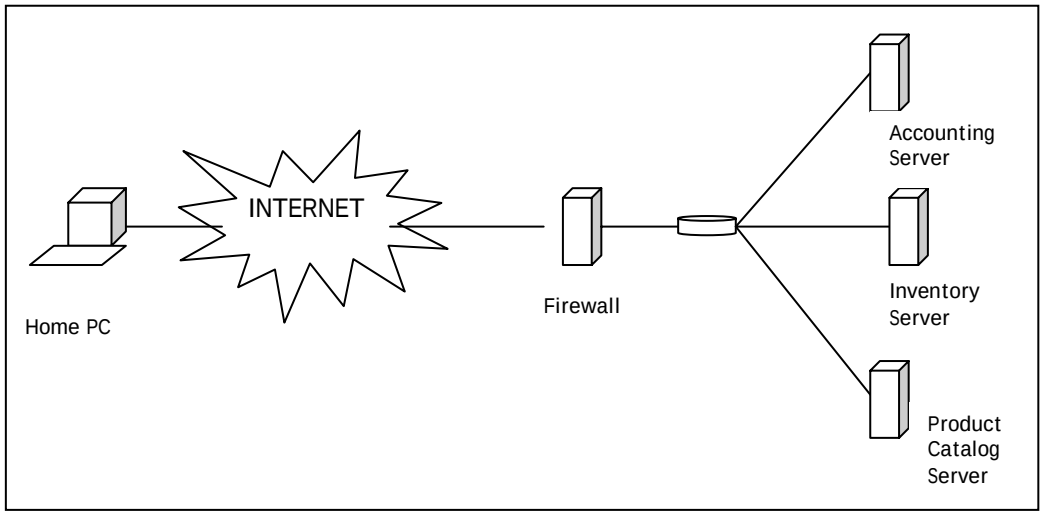
b. Sertifikat Digital (*Digital Certificate*)
Suatu metode juga diperlukan untuk memastikan bahwa seseorang benar-benar berasal dari suatu organisasi/perusahaan atau benar-benar jujur atas apa yang diklaim olehnya. Suatu sistem yang menggunakan sertifikat elektronik muncul untuk menjawab tantangan itu. Dalam sistem itu, sertifikat elektronik (berisi nama, organisasi, dan titel dan sebagainya) disimpan dalam sebuah basis data publik yang dapat dengan mudah diakses untuk memverifikasikan identitas seseorang dengan cepat. Sistem tersebut bekerja sebagai berikut.
   - Sebuah dokumen elektronik yang ditanda-tangani oleh pihak ketiga yang disebut Otorita Sertifikasi (*Certification Authority*).
   - Dokumen/Sertifikat itu berisi informasi mengenai seseorang atau sebuah organisasi seperti nama, lokasi, perusahaan, alamat *e-mail*, dan tanggal kedaluwarsa.
   - Setelah sertifikat itu ditandatangani oleh CA, dapat digunakan oleh pemegangnya sebagai bukti identitas.

Sertifikat Digital itu dapat dipakai untuk memverifikasi berbagai hal seperti menverifikasi public *key*, menverifikasi *e-mail*, menverifikasi situs, dan sebagainya. Perusahaan yang berperan sebagai pengesah sertifikat (CA), antara lain, Verisign (http://www.verisign.com) dan CertCo (http://www.cerco.com).

3. Metode yang Mendukung Keamanan Akses Komputer

Bila otentikasi diperlukan untuk menyaring orang yang mengakses suatu data, aplikasi atau jaringan baik dari dalam maupun luar sistem/jaringan komputer perusahaan, suatu metode lain diperlukan untuk menyaring data yang masuk ke dan keluar dari jaringan sistem informasi internal perusahaan. Disinilah teknologi *Firewall* berperan.

Tujuan dibangunnya *Firewall* untuk mengamankan jaringan internal yang lebih terpercaya (*trusted network*) dari jaringan luar yang kurang dipercaya (*untrusted network*) dengan cara memonitor data yang keluar masuk kedua jenis jaringan itu melalui satu titik akses. Secara lebih jelas, penempatan *Firewall* dapat dilihat pada diagram di bawah ini.



Gambar 4 Bagan Posisi *Firewall* dalam Jaringan Internal Perusahaan

Firewall sendiri dapat berupa *hardware* maupun *software* yang fungsinya, antara lain sebagai berikut.

1. Merekam lalu lintas data (*log traffic*) yang keluar masuk jaringan internal perusahaan.
2. Menyaring informasi. *Software* yang terpasang pada sebuah *Firewall server* dapat diprogram untuk menyaring paket data yang masuk dan keluar berdasarkan alamat IP, nama, *passwords*, dan sebagainya.
3. Mengontrol lalu lintas data. Hal itu merupakan fungsi yang lebih kompleks dan rumit ketika sebuah *firewall* melakukan identifikasi terhadap tingkat kewenangan akses serta memelihara sistem pelacakan kegiatan (*audit trail*) sehingga perusahaan dapat mengetahui profil dan kecenderungan dari para pemakai jaringan.

Banyak jenis dan tipe *firewall* yang ada dipasaran dewasa ini namun untuk menyingkatkan pembahasan variasi tersebut tidak disinggung lebih jauh.

4. Metode yang Mendukung Ketersediaan Pelayanan (*Availability*)

Metode keamanan transaksi juga menyangkut ketersediaan pelayanan secara terus-menerus dan hal itu dapat dicapai melalui berbagai cara antara lain sebagai berikut.

1. Membangun sistem *backup* untuk data dan aplikasi.
   Membangun sistem *backup* untuk data dan aplikasi dapat dilakukan dengan berbagai peralatan *backup* yang ada di pasaran, antara lain menggunakan *floppy disk*, CD, bahkan *hard disk* tambahan. Juga membuat duplikatnya secara manual dan teratur atau menggunakan sistem *backup* otomatis menggunakan **RAID** (*Redundant Array of Inexpensive Disk*), yaitu suatu sistem *backup* data menggunakan beberapa *hard disk* yang dihubungkan secara paralel sehingga data yang ditulis pada *hard disk* utama ditulis pula pada *hard disk* lainnya. Sistem itu biasa dipasang pada suatu *server*. Terdapat beberapa hal yang harus dipertimbangkan dalam melakukan *backup* terhadap data atau aplikasi, antara lain berikut ini.
   a. Pilihan media penyimpanan harus berdasarkan kapasitas dan volume pemakaian komputer yang di *backup*. Contohnya, penggunaan *floppy* atau CD cocok untuk komputer PC atau *workstation* sedangkan *server* sebaiknya di *backup* menggunakan *hard disk* tambahan atau RAID. Untuk *server* jenis *mainframe* atau *miniframe*, pemakaian media berkapasitas besar seperti *Magnetic Tape* dan *Disc* dapat dipertimbangkan.
   b. Lokasi penyimpanan media *backup* sebaiknya tidak berdekatan dengan komputer yang di *backup* karena bila terjadi musibah (kebakaran, gempa bumi, dan sebagainya) yang merusak fasilitas utama, media *backup* masih dapat diselamatkan.
   c. *Backup* data sebaiknya dilakukan secara rutin dan teratur dengan frekuensinya yang tergantung dari tingkat kepentingannya.
   d. Disarankan untuk membuat 3 duplikat data sehingga bila terjadi sesuatu kerusakan pada suatu duplikat data, masih dimiliki yang lainnya.
   e. Penggunaan *backup* data jarang terjadi dan hal itu mengakibatkan duplikat data jarang diakses dan dites sedangkan media penyimpanan data lama-kelamaan mengalami kerusakan sehingga dapat merusak data. Untuk mengantisipasi terjadinya hal itu maka *backup* data yang disimpan pada media penyimpanan harus dikopi ulang ke media baru setelah masa/periode kedaluwarsanya (menurut produsen media tersebut) tercapai.

2. Membangun sistem *backup* untuk fasilitas jaringannya sendiri.
   Selain data dan aplikasi, fasilitas jaringan juga perlu di*backup* demi mengantisipasi adanya bencana yang mengakibatkan rusaknya fasilitas tersebut. Cara yang populer adalah dengan membangun fasilitas komputer cadangan yang sewaktu-waktu dapat digunakan untuk menggantikan peran fasilitas utama yang rusak akibat suatu musibah. Ada tiga jenis fasilitas cadangan yang dapat dibangun, antara lain sebagai berikut.
   a. ***Cold Site*** adalah suatu fasilitas yang memiliki ruangan, sumber listrik, air, dan penerangan, serta ventilasi yang memadai namun tidak memiliki perangkat keras dan perangkat lunak. Tipe fasilitas jenis itu paling murah untuk dibangun namun paling lambat dalam hal menggantikan peran fasilitas utama.

b. ***Warm Site*** adalah suatu fasilitas yang selain memiliki ruangan, sumber listrik, air, penerangan, dan ventilasi juga memiliki perangkat keras (*hardware*) dan lunak (*software*) yang memadai untuk menggantikan peran fasilitas utama. Namun, kelemahan sistem itu adalah absennya *database* sehingga untuk mengoperasikannya masih memerlukan *database* yang dikopi dari sistem utama.

c. **Hot Site** adalah suatu fasilitas cadangan lengkap yang terdiri dari fasilitas listrik, air, penerangan, ventilasi, perangkat lunak, maupun keras ditambah dengan *database* yang di *update* secara berkala dari *database* pusat sehingga dapat dengan cepat menggantikan peran fasilitas utama.

5. Metode yang Mendukung Integritas Data

Metode keamanan yang mendukung integritas atau keutuhan data biasanya berupa metode yang telah dibangun di dalam suatu aplikasi (*software*) atau bahasa komunikasi data (*protocol*). Fungsi atau metode yang memastikan inetgritas suatu data biasa juga disebut fungsi kontrol dan fungsi kontrol yang disinggung dalam artikel ini adalah fungsi kontrol aplikasi (*application control*). Adapun fungsi kontrol dalam suatu aplikasi, antara lain sebagai berikut.

1. Kontrol dalam Pemrosesan (*Application Processing*). Fungsi Kontrol Pemrosesan itu meliputi proses pengecekan validasi, rekonsiliasi data, pengecekan nomor urut (*sequence*), dan identifikasi transaksi yang ganjil.
2. Kontrol terhadap Perkembangan Transaksi (*Transaction in Progress*). Fungsi itu mengecek penyelesaian suatu transaksi, apakah barang yang dipesan sudah dikirim atau belum.
3. Kelengkapan Data (*Data Completeness*), yaitu mengecek apakah data yang diterima utuh/lengkap atau tidak. Metode itu meliputi aktivitas membandingkan nilai *binary digit total* yang dihitung oleh komputer penerima dengan *binary digit total* yang disimpan pada paket data yang dikirim (*bit control check*).
4. Pelacakan Kegiatan akses data (*Audit Trail*). Suatu fungsi pelacakan terhadap aktivitas pengguna dalam mengakses dan memanfaatkan data. Hal itu perlu dilakukan untuk mengidentifikasikan dan melacak kegiatan akses dan pemanfaatan data yang tidak wajar.

Keempat fungsi/metode kontrol itu perlu dimiliki oleh suatu aplikasi manajemen basis data dan manajemen jaringan untuk menjamin integritas data, aplikasi, maupun jaringan sistem informasi secara keseluruhan.

6. Memilih Metode Pengamanan yang Tepat

Bila sudah menentukan metode pengamanan yang akan diterapkan berdasarkan justifikasi investasi yang telah dihitung rasionya, pertanyaan selanjutnya adalah bagaimana memilih produk keamanan yang tepat dari ratusan bahkan ribuan produk yang ada di pasaran. Tidak ada suatu kriteria yang pasti dalam memilih produk keamanan terbaik. Suatu produk yang berjalan baik pada jaringan komputer suatu perusahaan mungkin memperlihatkan kinerja yang buruk pada jaringan komputer perusahaan lainnya. Walau demikian, ada beberapa kriteria umum yang masih dapat dipakai untuk menilai ketepatan suatu produk untuk usaha.

Francis Pineda, seorang konsultan senior di bidang keamanan data dari I *Sentry Solutions Inc* menyatakan bahwa kriteria memilih produk keamanan yang ideal seharusnya mencakup factor, seperti berikut ini.

1. *Functionality*, apakah produk tersebut menawarkan fungsi keamanan yang diinginkan.

2. *Manageability*, apakah produk tersebut dapat dengan mudah dipasang, dioperasikan, dan dipelihara.
3. *Performance*, apakah produk tersebut mampu melakukan fungsinya dengan baik dan cepat walau menghadapi volume/beban pekerjaan yang tinggi.
4. *Value Added*, apakah produk tersebut menawarkan nilai tambah berupa fungsi dan fasilitas keamanan tambahan yang diperlukan atau berpotensi untuk diperlukan dimasa mendatang.
5. *Support*, apakah produk keamanan tersebut mendapat dukungan penuh dari pembuatnya dalam hal perbaikan (*maintenance*), penyempurnaan (*upgrade/improvement*), dan penggantian (*replacement*).
6. *Warranties*, apakah produk tersebut dijamin dapat melakukan seluruh fungsi dan kemampuan yang diklaim pembuatnya.
7. *Cost*, apakah harga produk tersebut sesuai dengan dana yang dianggarkan perusahaan atau sesuai dengan fasilitas dan fungsi yang ditawarkannya.

PENUTUP

Simpulan

Biaya mengamankan transaksi lewat internet memang mahal dan biayanya akan kelihatan semakin mahal bila perusahaan tersebut belum pernah mengalami serangan terhadap sistem dan jaringan komputernya. Namun demikian, pengamanan itu perlu dilakukan bila ingin memanfaatkan internet sebagai sarana berbisnis karena cepat atau lambat seiring dengan meningkatnya kemampuan dan daya beli masyarakat di negara berkembang, internet akan menjadi salah satu sarana untuk berbelanja. Bila pengusaha tidak mau terlibas oleh persaingan global maka mereka pun harus siap untuk merambah dunia *cyber* dan meramaikan industri *e-business* global dengan terlebih dahulu menjamin keamanan bertransaksi dengan melakukan serangkaian investasi bertahap sesuai dengan kebutuhan bisnis dan kemampuan pendanaan masing-masing. Meniru kata Neil Amstrong ketika menginjakkan kakinya di bulan "*A little step for a local business….. a giant leap to e-business* "

DAFTAR PUSTAKA

Bayan, Ruby. 2004. "*How to Choose the Best Security Solution*." ZDNET online publication, URL: Http://www.zdnet.com.au/insight/0.39023731.20282525.00.htm

Fink, Dieter. 1998. *E-Commerce Security*. Australian Print Group.

Radcliff, Deborah. 2002. *Choosing The Best Security Guards: IT Tackles Management Issues Via Service Providers*. Computerworld Publication.

Turban, Efraim. 2002. *Electronic Commerce A Managerial Perspective*. Prentice Hall.