Metode Pengamanan Jaringan pada Model Kerja e-Government [1]

Oleh :
Julio Adisantoso [2]

Pada dasarnya kita semua menginginkan privasi, keamanan, dan perasaan aman dalam hidup, termasuk dalam penggunaan jaringan komputer.

Dalam beberapa tahun belakangan, perkembangan dan penggunaan teknologi jaringan komputer, khususnya Internet, pesat sekali. Semakin banyak saja kalangan bisnis, organisasi, perkantoran, pendidikan, militer, hingga individu menggunakan jasa teknologi informasi ini yang lebih sering dikenal dengan "*The Information Superhighway*". Sejalan dengan laju pertumbuhan penggunaan teknologi informasi yang sangat cepat, maka semakin banyak pula aplikasi-aplikasi yang dibutuhkan oleh pengguna, seperti pada aplikasi di dunia perdagangan bebas secara elektronik (*electronic commerce*), pendidikan (*electronic education*), penyelenggaraan pemerintahan (*electronic government*), dan sebagainya.

ELECTRONIC GOVERNMENT (e-Government)

Seiring dengan perkembangan yang sangat cepat dalam *digital economy*, pemerintah secara bersamaan mencoba menerapkan suatu teknologi yang diasumsikan akan merubah pola layanan, mengurangi biaya dan waktu yang biasa terjadi pada model administrasi *paper-based*. Selain itu pemerintah secara terus menerus mencoba meningkatkan partisipasi aktif masyarakat dalam pencapaian tujuan negara.

E-Government mencakup semua usaha untuk meningkatkan kualitas pelayanan pemerintahan kepada masyarakat, termasuk di dalamnya adalah peningkatan efektifitas dan efisiensi penyelenggaraan pemerintahan, dengan memanfaatkan teknologi informasi. Misalnya, masyarakat umum seharusnya bisa mendapatkan layanan tertentu (KTP, surat pindah, dan sebagainya) dalam hitungan menit atau jam, bukan lagi dalam hitungan hari

[1] Disampaikan pada Seminar e-Government dalam Unsri Computer Fair 2003 di Palembang, 24 Mei 2003
[2] Kepala UPT Komputer IPB dan Staf Pengajar Jurusan Ilmu Komputer FMIPA IPB

apalagi minggu. Hal yang sama dapat juga dilakukan untuk proses-proses pemerintahan yang lain, misalnya dalam hubungannya dengan para pelaku bisnis atau bahkan antar entitas pemerintahan itu sendiri.

Paling tidak ada 4 hal yang menjadi sasaran pengembangan e-Government, yaitu:

1. Layanan individual/warga negara atau *Government to Citizens* (G2C). G2C membangun fasilitas satu pintu yang mudah ditemui dan mudah digunakan untuk semua layanan pemerintahan kepada warga negara.
2. Layanan Bisnis atau *Government to Bussiness* (G2B). G2B mengurangi beban kerja pengontrolan bisnis (misalnya pelaporan keuangan perusahaan pada pemerintah, penghitungan pajak, dan sebagainya) dengan cara menghilangkan duplikasi pengumpulan data.
3. Antar entitas pemerintahan atau *Government to Government* (G2G) G2G memudahkan penyelenggara pemerintahan lokal untuk mendapatkan data dari partnernya (misalnya pemerintah lokal yang lain).
4. Internal pemerintahan atau *Internal Efficiency & Effectiveness* (IEE) memanfaatkan teknologi informasi untuk mengurangi biaya administrasi pemerintahan dengan menggunakan alat bantu yang sudah teruji efektifitasnya di dunia bisnis seperti supply chain management, financial management dan *knowledge management*.

PENGAMANAN SISTEM

Dalam pengembangan e-Government, perlu dipersiapkan beberapa hal antara lain:

1. Kebijakan pemerintah.
2. Penumbuhan budaya yang mendukung pada unit-unit penyelenggara pemerintahan.
3. Rasionalisasi struktur data dan penyelenggara pemerintahan agar sesuai dengan kebutuhan e-Government (misalnya: mengusahakan agar tidak ada data yang terduplikasi antar entitas pemerintahan)
4. Penyiapan mekanisme "*online trust*" melalui pengamanan sistem komputer
5. Penyiapan sumber daya manusia.

6. Penyiapan strategi untuk mengatasi resistensi dari orang-orang yang berkepentingan.

Empat hal yang disebut di atas merupakan butir penting yang harus mendapat prioritas pengembangan e-Government, yang di dalamnya mencakup pengamanan sistem. Aspek pengamanan jaringan komputer (*computer network security*) menjadi sangat populer dan penting serta merupakan suatu keharusan atau kebutuhan mutlak.

Faktor keamanan sistem juga merupakan salah satu agenda utama bagi e-Government yang memiliki proses terkait dengan *on-line transaction* tanpa membocorkan informasi pribadi atau informasi sensitif lainnya yang dimiliki oleh masyarakat dan komponen bisnis. Proses penjaminan keamanan ini sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dan dunia bisnis terhadap sistem e-Government yang sedang diimplementasikan oleh suatu negara.

Pengamanan sistem e-Government tidak terlepas dari pengamanan jaringan komputer dan Internet secara umum karena pengembangan jaringan komputer dan Internet dinilai sebagai awal model penerapan e-government secara penuh oleh lembaga pemerintah di pusat dan daerah. Pengembangan e-government dapat dimulai dengan pembangunan situs yang menyediakan peluang untuk pooling atau mekanisme interaksi, penyediaan pelayanan administratif untuk perijinan atau yang terkait dengan sistem persyaratan tertentu.

PERLUNYA PENGAMANAN SISTEM

Komputer yang terhubung ke jaringan sangat potensial diakses oleh pengguna yang tidak berhak, atau yang sering disebut sebagai ”*hacker*s”. Berdasarkan hasil riset dan survei serta berbagai laporan tentang kejahatan komputer yang terjadi dewasa ini, diketahui bahwa tidak ada satu pun jaringan komputer yang diasumsikan 100 persen aman dari serangan virus komputer, *spam*, *e-mail bomb*, atau diterobos langsung oleh para *hackers*. Sangat sulit mencari angka yang pasti tentang peristiwa kejahatan seperti ini karena

banyak menyangkut publikasi negatif pada suatu sistem jaringan. Berikut adalah sekedar ilustrasi:

- 1996. *FBI National Computer Crime Squad, detected computer crime 15%, only 10% of that number is reported*.
- 1996. *American Bar Association: survey of 1000 companies, 48% experienced computer fraud in the last 5 years*.
- 1996. *United Kingdom, NCC Information Security Breaches Survey: computer crime increased 200% from 1995 to 1996*.
- 1997. *FBI: computer crime case in court increased 950% from 1996 to 1997, convicted in court increased 88%*.

Masih berdasarkan catatan statistic, para pelaku kejahatan computer menurut CSI/FBI Computer Crime and Security Survey pada tahun 1999 adalah:

1. Disgruntled employees 86%
2. Independent hackers 74%
3. Competitors 53%
4. Foreign Corporations 30%
5. Foreign Governments 21%

Bagaimana dengan di Indonesia? Banyak sekali situs-situs di Indonesia yang sudah pernah "diobok-obok" oleh para vandal, dan pernah tersiar berita bahwa ada *cracker* Indonesia yang tertangkap di Singapura. Disamping itu, berdasarkan statistic kejahatan komputer, Indonesia masuk dalam ranking (2%) yang mencoba melakukan *attack* terhadap situs web di luar negeri, terutama Amerika Serikat.

Berdasarkan data tersebut, muncul berbagai pertanyaan terkait dengan pengamanan system jaringan computer seperti: Apakah jaringan computer itu cukup aman? Apakah aman bila melakukan proses perijinan melalui jaringan computer tanpa khawatir seseorang mencuri informasi tentang perusahaan yang akan dibangun? Apakah mungkin seseorang mengetahui password orang lain dan menggunakannya tanpa ketahuan?

Dapatkah sesorang mencuri atau memanipulasi file orang lain? Dapatkah kita mempunyai sebuah jalur komunikasi yang aman di Internet? Apa yang harus dilakukan untuk mengamankan sistem jaringan komputer? dan sebagainya. Untuk menjawab

semua pertanyaan tersebut sangatlah tergantung dari tingkatan permasalahannya sendiri, yang sangat tergantung kepada setiap kasus yang terjadi.

Pada dasarnya kita semua menginginkan privasi, keamanan, dan perasaan aman dalam hidup, termasuk dalam penggunaan jaringan komputer. Kita mengharapkan hasil pekerjaan kita aman dan jauh kemungkinan untuk dicuri, di-*copy*, atau dihapus. Kita juga menginginkan keamanan pada waktu saling kirim e-mail tanpa khawatir ada pihak tidak bertanggung jawab (*malicious users*) yang dapat membaca, mengubah atau menghapus isi berita e-mail tersebut.

Pengamanan juga diperlukan sebagai akibat tidak dapat dijaminnya suatu sistem 100% akan bebas dari kerusakan fisik seperti kerusakan media penyimpanan (hard-disk), kerusakan sistem, bencana alam, dan sebagainya.

METODE PENGAMANAN

Langkah yang umum dilakukan pada implementasi e-Government adalah penjaminan layanan elektronik yang menyediakan akses melalui portal dan *secure gateway* bagi seluruh stake holder pemerintahan. Beberapa metode pengamanan yang dapat dilakukan adalah pengaturan :

1. ***Authentication***, Pemahaman tentang personal dan jenis perangkat yang dipergunakan untuk mengakses sistem. Hal yang menjadi perhatian utama dalam proses *authentication* adalah :
   - Komponen informasi yang diketahui pengguna, seperti password atau nomor PIN
   - Komponen informasi yang dimiliki oleh pengguna, seperti smart card atau *hardware token*.
   - Komponen informasi yang secara natural dimiliki oleh pengguna, seperti fingerprint atau *iris scan*.

   Satu hal yang perlu diingat bahwa model *authentication* bukan suatu metode pengamanan tunggal, melainkan salah satu bagian dari metode pengamanan modul e-Government.

Beberapa alternatif implementasi yang dapat dipilih pada proses online atuhentication diantaranya :

- ***Passwords, personal identification number (PINs)*** **dan** ***user identification*** **(User ID).**

  Metode ini adalah model yang paling umum dipergunakan pada *on-line transaction*, terdapat beberapa hal penting yang menjadi kunci utama keberhasilan model authentication ini, yaitu :

  - Panjang karakter ID (diperlukan manajemen jumlah minimum karakter bagi password
  - Penggunaan verifikasi dengan model kamus bahasa, hal ini memaksa pengguna untuk tidak menggunakan serangkaian karakter yang terdefinisi sebagai suatu kalimat dalam kamus.
  - Penerapan waktu kadaluarsa
  - Pencatatan waktu login untuk proses audit sangat menguntungkan untuk penelusuran suatu tidak kejahatan dalam sistem.

- ***One-time password***.
  Seringkali kata password terlupakan oleh pengguna, hal ini merupakan suatu yang cukup riskan bagi metode pengamanan suatu aplikasi. *One-time password* mencoba mengeliminasi resiko ini dengan mempergunakan perangkat keras yang mampu membangkitkan kode unik setiap pengguna memasuki aplikasi. *Token password* dibangkitkan dengan model *symmetric key* yang hanya akan valid pada saat itu saja.

- ***Challenge and response system***
  Model authentication ini dapat diimplementasikan dengan menggunakan cara manual (dengan form register) dan secara otomatis (menggunakan perangkat keras atau token). Secara manual pengguna akan memasukan ID dan password, selanjutnya sistem akan secara acak menanyakan suatu informasi dari biodata yang terdapat dalam form registrasi. Sedangkan Proses secara otomatis melibatkan asymmetric cryptography dan user mempergunakan perangkat keras pembangkit sandi yang unik sesuai dengan yang diisukan oleh sistem.

- ***Cookies***
  Cookies adalah serangkaian informasi yang disimpan secara lokal dalam sistem pengguna. Informasi ini dikirimkan oleh situs web yang diakses oleh pengguna dan akan tersimpan serta valid dalam jangka waktu tertentu.

- ***Biometrics***
  Teknologi *biometric* menggunakan suatu ciri fisika atau karakteristik tertentu yang dimiliki oleh pengguna sistem. Sebagai contoh adalah : *Iris*

Scan, *Retina scan*, *Finger scan*, *hand geometry*, *voice verification* dan *dynamic signature verification*. Seluruh metode tersebut mencoba menyajikan ciri fisik manusia ke dalam bentuk informasi digital yang dapat diinterpresikan oleh sistem serta dapat di identifikasi secara unik.

- ***Conventional encryption***
  Contentional encryption adalah suatu algoritma yang bekerja menyandikan suatu text. Beberapa referensi menyebutnya sebagai '*symmetric cryptography*' sistem menggunakan *secret key*, dimana melibat perhitungan matematik untuk melakukan proses enkripsi dan dekripsi dari element informasi. Kelemahan dari metode ini adalah dari sisi pengguna diharuskan selalu menyimpan secret key untuk setiap transaksi sehingga dibutuhkan mekanisme distribusi yang aman, hal ini tentunya membutuhkan sumberdaya yang tidak sedikit.

- ***Public key crytography* (*digital ceritificates*)/*Public key infrastructure* (PKI)**
  Permasalahan pendistribusian *secret key* yang terjadi pada model *conventional encryption* dapat diselesaikan dengan penggunaan *public key cryptography*. *Public key crypthography* menggunakan pasangan kunci terpisah untuk melakukan proses validasi. Pasangan kunci ini dinyatakan sebagai *public key* dan *private key*. *Public key* berfungsi menangani proses enkripsi dengan cara sebagai berikut: Pada saat penggunakan pasangan kunci authentication, pengguna menyebarkan informasi *public key* ke seluruh komponen sistem, jika terdapat sebuah modul sistem yang memiliki *public key* yang sama maka modul sistem mampu mendekripsi *public key* yang dikirim serta memberikan penjaminan untuk pengiriman *private key* yang dipergunakan pada proses dekripsi level berikutnya.

- ***Pretty good privacy* (PGP)**
  PGP adalah sebuah aplikasi enkripsi yang diperuntuk bagi sekelompok kecil orang yang ingin bertukar informasi secara aman. Proses ini sepenuhnya dilakukan dengan pertukaran *private key* di antara sesama pengguna.

- ***Secure socket layer* (SSL) dan *Transport Layer Security* (TLS)**
  SSL protokol adalah satu set aturan komunikasi yang sepenuhnya disandikan dan hanya dapat dipahami oleh pengguna dan server yang sedang berkomunikasi. Protokol ini dikembangkan untuk mengamankan transmisi data penting pada jaringan internet.

2. ***Authorization***, pemahaman tentang sumberdaya apa yang tersedia untuk pengguna dan perangkat yang telah lulus proses validasi. Proses ini sepenuhnya diserahkan pada tahapan identifikasi kebutuhan sistem dan identifikasi komponen yang terlibat dalam desain e-Government.

3. **Pengamanan Sistem Jaringan,** Pada lapisan terakhir ini diperlukan pengamanan lebih serius, hal ini disebabkan sistem jaringan merupakan tulang punggung komunikasi bagi seluruh modul e-government. Beberapa implementasi fisik yang dapat dilakukan adalah:

    - **Firewall**
      Firewall adalah sebuah system proteksi untuk melaksanakan pengawasan lalu lintas paket data yang menuju atau meninggalkan sebuah jaringan komputer sehingga paket data yang telah diperiksa dapat diterima atau ditolak atau bahkan dimodifikasi terlebih dahulu sebelum memasuki atau meninggalkan jaringan tersebut.

    - **Intrusion Detection System**
      Sistem ini akan mendeteksi pola atau perilaku paket data yang masuk ke jaringan untuk beberapa waktu sehingga dapat dikenali apakah paket data tersebut merupakan kegiatan dari pihak yang tidak berhak atau bukan.

    - **Network Scanner**
      Scanner adalah sebuah program yang secara otomatis akan mendeteksi kelemahan-kelemahan (*security weaknesses*) sebuah komputer di jaringan local (*local host*) maupun komputer di jaringan dengan lokasi lain (*remote host*).

    - **Packet Sniffing**
      Program ini berfungsi sebagai alat untuk memonitor jaringan komputer. Alat ini dapat diperasikan hampir pada seluruh tipe protokol seperti Ethernet, TCP/IP, IPX, dan lain-lain.

EVALUASI ASPEK KEAMANAN JARINGAN

Secara teknis sangat sulit untuk mengevaluasi sebuah jaringan komputer secara spesifik. Itu semua tergantung pada banyak hal, antara lain banyaknya jumlah user atau client dalam jaringan komputer dengan berbagai access point yang ada, model jaringan, jenis dan versi sistem operasi yang digunakan, dan keahlian, kemahiran serta pengetahuan dari *system administrator* atau *network administrator*.

Prosedur yang sederhana dan mudah untuk mengevaluasi aspek keamanan jaringan komputer dalam model kerja e-Government adalah dengan memanfaatkan seluruh program-program atau utiliti-utiliti mengenai *hacking* (*hacking tools*) yang ada. Program

ini dicobakan pada jaringan komputer sehingga dapat dilihat seberapa parah dampak negatif yang akan ditimbulkan.

Beberapa program atau *utility* tersebut antara lain IP Scanner, IP Sniffer, Network Analyzer, Email Bombs, Spamming, TCP Wrapper, Password Cracking, dan sebagainya. Dengan cara ini segera dapat dilihat kemampuan pengamanan dan keamanan jaringan computer yang sering disebut sebagai "*security holes*" atau "*back doors*".

PENUTUP

Peralatan dan metode telah tersedia dalam jumlah yang memadai untuk mengamankan suatu system jaringan, termasuk dalam model kerja e-Government. Namun demikian, tidak semuanya dapat dipergunakan secara efektif karena sesuatu yang kita anggap aman untuk saat ini akan terbukti menjadi tidak aman lagi pada masa yang akan datang. Oleh karena itu, peran *network administrator* sangat penting dalam menjaga keamanan system secara keseluruhan.

Beberapa hal yang dapat dilakukan untuk mengantisipasi serangan penyusup atau kerusakan sistem antara lain:

1. ***Backup Computer Data***
   Melaksanakan backup data secara reguler (harian, mingguan, atau bulanan) untuk mengantisipasi bila terjadi kerusakan atau kehilangan seluruh data sehingga dengan mudah dan cepat dapat dilakukan recovery seluruh sistem.

2. ***Minimize Network Access***
   Tidak semua user maupun aplikasi selalu terhubung ke jaringan, sehingga perlu ada pembatasan atau minimal pengelompokan sistem jaringan.

3. ***Use Strong Password***

4. ***Access Rules***
   System Administrator harus rajin menginformasikan kepada seluruh user mengenai hak dan kewajibannya dalam menggunakan jaringan sebagai pendukung utama suatu model kerja e-Government. Para user perlu diinformasikan bagaimana cara yang benar menggunakan jaringan komputer secara aman seperti cara membuat password yang baik, mengingatnya, dan sebagainya.

REFERENSI

1. Network Security. http://pangea.standord.edu/computerinfo/network/security.

2. Membangun e-Government. http://www.geocities.com/seminartc.

3. Aspek Pengamanan dalam Dunia E-Commerce. http://www.cert.or.id

4. Amankah Jaringan Komputer dan Internet Anda? Sebuah Kisah yang Tanpa Akhir. Rudy AG Gultom. Kompas Senin, 12 Mei 2003.

5. Using IEEE 802.1x to Enhance Network Security. Foundry Networks. Anton James, 2002.

6. Network Security for the Small Business: An Insight. http://www.3com.com.

7. Overview of Network Security. Budi Rahardjo, 2002.

8. Authenticated Transmission Using A Non-Cryptographic Approach. Fan Du and Lionel Ni, 2002.

9. Network Security Policy: Best Practice. http://www.cisco.com/warp/public/126.

JULIO ADISANTOSO

Kepala UPT Kompter IPB
Gedung Rektorat Lt. 2 Kampus IPB Darmaga, Bogor.
Telp/Fax : +62-251-623936 | 622642 etx. 101

Ketua Program Studi S1 Ilmu Komputer
Fakultas Matematika dan IPA, Institut Pertanian Bogor
Kampus IPB Baranangsiang, Jl. Raya Pajajaran Bogor
Telp/Fax : +62-251-356653