Mengamankan Bagian yang Sering Terlupakan Dalam Keamanan Jaringan

Jim Geovedi
negative@toxic.magnesium.net

Fakta di sekitar kita

Internet, tanpa disadari telah mengubah cara orang bekerja, berkomunikasi, bekerjasama, melakukan kegiatan jual dan beli, bersosialisasi, dan lain-lain. Pemberian akses yang terkontrol kepada mitra adalah hal yang paling praktis sebagai upaya mempermudah kerjasama kedua-belah pihak. Namun dengan mengijinkan mitra menjelajah lebih dalam pada jaringan perusahaan yang mengaburkan batasan antara luar dan dalam? Saya tidak percaya jika ada sebuah perusahaan yang bersedia jika rahasia dapurnya diketahui oleh orang lain.

Anggapan tradisional tentang keamanan jaringan mengasumsikan bahwa koneksi dibelakang firewall adalah aman dan koneksi diluar firewall adalah rawan, tidak mampu menjamin bahwa aset berharga perusahaan dapat terlindungi dengan baik. Saat ini jaringan bisnis berskala besar membutuhkan keamanan yang mampu mengamankan sampai kesemua *end-points* baik yang berada di dalam maupun di luar lingkup jaringan perusahaan.

Dibalik perlindungan Firewall

Perlindungan Firewall konvensional hanya melindungi bagian dalam dari jaringan. Firewall akan memfilter serta mengaudit traffic yang melintasi perbatasan antara jaringan luar maupun dalam. Bagaimanapun, Firewall tidak

dirancang untuk melindungi koneksi individu dalam sebuah jaringan. Hal ini dapat dianalogikan sebagai mengunci pintu gerbang, namun tidak membiarkan pintu masuk kedalam rumah atau pintu kamar - siapapun yang berhasil masuk melewati pintu gerbang, tentunya akan sangat mudah menjelajah isi ruangan.

Tipe jaringan seperti diatas sangatlah berisiko tinggi sebagai *attack target*. Sebagai contoh, seorang *attacker* yang mengincar server atau workstation yang terletak dalam jaringan internal (*LAN - Local Area Network*), begitu ia mendapatkan akses masuk ke mesin tersebut, mereka dapat menggunakannya sebagai *jumping box* untuk menjebol masuk ke sistem lain yang berada di dalam jaringan yang sama.

Cara yang dapat ditempuh untuk menyiasati kondisi tersebut adalah dengan mengunci setiap ruangan. Kurang lebih sama seperti solusi yang ditawarkan firewall yang diperuntukkan pada desktop, notebook, atau server yang berada dalam LAN. Dengan memasang firewall pada titik-titik rawan dapat memberikan kemudahan akses pada pengguna untuk memperoleh atau menempatkan informasi-informasi penting. Dengan metode *end-to-end security* ini, tidak akan menimbulkan masalah apabila pengguna terhubung dalam intranet, extranet, VPN atau remote access. Metode tersebut juga dapat mencegah *intrusion* pada sebuah host untuk menyebar ke host lain yang *restricted-access* pada network yang sama.

Kontrol keamanan

Walaupun semua perusahaan seharusnya memahami soal keamanan jaringan, beberapa harus memberikan perhatian yang lebih. Mereka yang menyimpan atau mendistribusikan data penting membutuhkan solusi yang lebih rumit. Mereka yang membutuhkan solusi ekstra diantaranya adalah institusi keuangan, pemerintahan, jasa asuransi, pengembang, dan rumah-sakit.

Ada banyak dari mereka yang sudah terhubungkan melalui jaringan - baik private maupun via Internet - ke kantor cabang, mitra kerja, sehingga pertukaran informasi dapat menjadi sangat mudah. Sebagaimana jaringan

yang berkembang menjadi sangat distributif, solusi keamanan jaringan harus ikut menyesuaikan diri. Melengkapi hardware dengan solusi keamanan ekstra - menempatkan kunci tambahan pada setiap pintu ruangan - menjadi opsi yang konsisten, hal tersebut terdengar seperti sudah menjadi kebijakan keamanan antar jaringan.

Untuk perlindungan secara fisik, hardware dapat dilengkapi dengan *crypto-card*, atau *biometric scanner* – scanner yang dapat mengenali siapa saja yang berhak mengakses berdasarkan anatomi tubuh seperti retina mata, sidik jari, dan suara. Sedangkan solusi dengan menggunakan software, dapat berupa personal firewall dan anti-virus scanner.

Perlindungan secara kontinyu

Sering saya mendengar beberapa rekan yang mengeluh karena jaringan yang menurut mereka sudah aman, ternyata masih dapat disusupi oleh *crackers*. Saya pikir dengan menyerahkan begitu saja tugas menjaga keamanan kepada software atau hardware, tidak dapat menyelesaikan masalah yang timbul. Perlu dilakukannya auditing secara berkala - secara lebih spesifik, *security audit* - untuk memeriksa cacat yang ada pada software atau hardware. Jika dirasa mampu, mungkin dengan mempekerjakan tenaga profesional yang ditugaskan untuk mengaudit keamanan jaringan, dapat meringankan beban Anda.

Selain itu, ada hal lain yang dirasa penting: beri pemahaman kepada karwayan - terutama mereka yang menggunakan jaringan - agar mengerti soal keamanan jaringan! Mereka adalah salah satu kunci yang tidak boleh terlupakan. Karyawan yang tidak memahami benar soal keamanan data dan jaringan akan menjadi bumerang bagi perusahaan.

Sebagai ilustrasi nyata, beberapa waktu yang lalu, saya menerima e-mail dari seseorang yang tidak saya kenal, dimana pada e-mail tersebut disertakan attachment berisi data pegawai perusahaan Y - berikut daftar gaji, anggota keluarga, pendidikan terakhir, dan lain sebagainya. Data yang menurut saya adalah data penting dimana tidak sembarang orang boleh tahu. E-mail terse-

but tentu tidak mungkin dikirimkan dengan sengaja, e-mail terkirim sebagai akibat terinfeksinya komputer sipengirim oleh Worm.

Menurut saya, terjadinya kebocoran informasi seperti yang baru saya sebut diatas, tidak mungkin terjadi jika pengguna adalah seseorang yang memahami benar soal keamanan data, karena ia akan melindungi data penting yang disimpannya dengan baik, juga akan memasang anti-virus - sudah tentu rajin meng*update*nya. Sungguh, sangat disayangkan sekali hal itu dapat terjadi.

Sedikit paranoid itu perlu

Dengan semakin seringnya tersiar isu keamanan jaringan, tidak mengherankan bagi perusahaan-perusahaan besar yang sudah terintegrasi dengan jaringan - menggunakan LAN, VPN, atau Internet - akan benar-benar mempertimbangan isu tersebut demi berlangsungnya bisnis yang tengah berjalan.

Sebagaimana *crackers* dan penulis virus/worms semakin cerdik, maka tingkat kewaspadaan harus semakin ditingkatkan. Penggunaan produk keamanan jaringan mungkin akan menjadi sebuah keharusan. Telah tersedia banyak dipasaran, produk personal firewall dan anti-virus yang dapat diintegrasikan kedalam notebook, desktop, dan server yang menjadikan sistem lebih aman dan terkendali.

Mereka yang menghendaki keamanan ekstra sebaiknya meminta vendor untuk mengintegrasikan firewall untuk mengamankan bagian yang sering terlupakan dalam keamanan jaringan: **personal computer**.