Budi Rahardjo

Arsitektur Keamanan Teknologi Informasi

Masalah keamanan (*security*) yang terkait dengan teknologi informasi mulai mendapat perhatian yang lebih serius dibandingkan sebelumnya. Salah satu penyebab hal ini adalah adanya banyak kasus yang terkait dengan keamanan yang dihadapi oleh perusahaan. Namun ternyata, penanganan masalah keamanan ini masih bersifat reaktif dan tidak terstruktur. Ada keinginan untuk membuat penanganan yang lebih tertata dengan rapi. Istilah yang populer untuk hal ini adalah membuat sebuah arsitektur keamanan (*security architecture*).

Untuk memahami hal ini, mari kita ambil analogi dengan melihat arsitektur bangunan. Ada banyak orang yang membuat rumah tanpa disertai dengan desain arsitektur yang terdokumentasi dengan baik. Rumah dibuat asal memenuhi kebutuhan fungsional. Di rumah tersebut ada kamar tidur, ruang tamu, dapur, dan kamar mandi. Beberapa waktu kemudian, ternyata tingkat ekonomi pemilik rumah menjadi lebih makmur dan sanggup membeli sebuah mobil. Maka kemudian dibuat garasi yang menempel di bagian samping rumah tersebut. Anak-anak makin besar sehingga membutuhkan kamar sendiri. Maka ditambahkan kamar di bagian belakang. Ternyata kondisi keamanan di sekitar rumah juga memburuk sehingga perlu dipasang pagar. Penambahan ini terus berlangsung dan bersifat asal jadi sehingga berkesan kumuh.

...penanganan masalah keamanan ini masih bersifat reaktif dan tidak terstruktur.

Hal yang sama juga terjadi di dunia teknologi informasi di banyak perusahaan. Jaringan tumbuh tanpa terkendali sesuai dengan peningkatan jumlah pekerja. Server juga bertambah sesuai dengan adanya layanan baru. Kemudian jaringan di kantor dihubungkan dengan Internet dan mulai timbul masalah keamanan.

Kembali kepada masalah desain bangunan, tidak semua bangunan memiliki fitur keamanan yang sama. Desain arsitektur sebuah rumah untuk keluarga kecil tentunya berbeda dengan desain arsitektur sebuah hotel atau perkantoran dengan penghuni ratusan orang. Sisi keamanannya pun juga berbeda.

Pengamanan di sebuah hotel lebih kompleks daripada pengamanan sebuah rumah biasa. Jumlah pegawai yang cukup banyak dan tamu yang keluar masuk merupakan sebuah tantangan tersendiri. Pegawai pun memiliki wewenang yang berbeda-beda, mulai dari *front desk, bell boy,* dapur, pembersih kamar, sampai ke satpam. Repotnya, satuan pengamanan pun tidak boleh masuk ke kamar sembarangan. Ini semua diatur dengan prosedur. Arsitektur keamanan teknologi informasi untuk sebuah perusahaan mirip dengan keamanan di hotel tersebut.

Arsitektur keamanan teknologi informasi memiliki beberapa komponen, yaitu (1) kumpulan sumber daya yang tersentralisasi (*centralized resource*), (2) pengelolaan identitas (*identity management*), (3) sistem otorisasi (*authorization system*), (4) *access control,* (5) pengelolaan kebijakan (*policy management*), (6) sistem pemantau (*monitoring system*), (7) *security operation*, (8) intranet yang aman (secure intranet / LAN), dan (9) Internet yang aman (secure Internet). Masing-masing komponen ini perlu mendapat pembahasan sendiri-sendiri. Untuk kali ini kita bahas komponen yang pertama, yaitu kumpulan sumber daya.

Sumber daya (*resources*) merupakan aset dari perusahaan yang ingin dilindungi. Dia bisa berupa perangkat keras, perangkat lunak, dan yang lebih penting adalah data serta informasi yang berada di dalamnya. Di beberapa perusahaan, sumber daya ini tersebar di beberapa tempat sehingga menyulitkan pengamanannya.

Tren yang ada saat ini adalah secara fisik mengumpulkan server-server (yang di dalamnya berisi aset) di sebuah pusat data (*data center*). Secara logik pun server-server ini dikelompokkan dalam beberapa kumpulan. Ada kumpulan server yang membutuhkan tingkat keamanan sangat tinggi, sementara itu ada juga kumpulan server yang pengamanannya tidak perlu tinggi sekali karena akan menjadi sangat mahal biaya operasionalnya. Untuk layanan yang berhubungan dengan publik biasanya kumpulan server tersebut dijadikan satuan di daerah DMZ (*demilitarized zone*), yang biasanya berada di belakang *firewall.*

Kesulitan yang dihadapi dalam menyatukan aset ini adalah ego dari pemilik aplikasi dan data yang ingin mengelola sendiri. Akhirnya server menjadi tersebar, menyulitkan pengelolaan, dan membutuhkan biaya yang lebih besar. Upaya untuk penyatuan ini membutuhkan keterbukaan dan perubahan kultur. Ayo kita satukan sumber daya kita demi kepentingan perusahaan.