

Secure Intranet

Melanjutkan pembahasan arsitektur keamanan, salah satu komponen dari arsitektur tersebut adalah adanya *secure intranet*. Pengelola jaringan sering terjebak oleh pandangan bahwa serangan terbesar terhadap sistem mereka berasal dari Internet. Padahal kenyataannya, orang dalamlah yang memiliki potensi terbesar sebagai ancaman. Statistik dari berbagai sumber menunjukkan bahwa orang dalam memiliki potensi terbesar, atau nomor dua terbesar, sebagai penyerang.

Hal ini dapat dimengerti karena orang dalam lebih mengetahui apa saja aset dari organisasi dan di mana letak aset tersebut. Mereka juga lebih dekat ke aset tersebut, atau bahkan ada yang memiliki akses kepada aset tersebut sebagai bagian dari pekerjaan sehari-hari. Inilah sebabnya pengamanan jaringan intranet harus mendapat perhatian juga.

Repotnya, pengamanan dari orang dalam lebih susah daripada pengamanan terhadap penyerang dari luar. Untuk penyerang dari luar kita bisa memisahkan jaringan kita dengan menggunakan *firewall*. Apakah *firewall* bisa kita gunakan juga untuk mengamankan jaringan intranet? Sebetulnya bisa, akan tetapi pendekatan ini tidak populer. Jadi bagaimana? Ada beberapa hal yang dapat dilakukan untuk meningkatkan pengamanan intranet.

Segmentasi jaringan—dengan berbagai cara seperti membatasi routing, menggunakan VLAN, dan bahkan menggunakan *firewall*—merupakan sebuah langkah yang harus dilakukan untuk mengamankan intranet. Jaringan tidak boleh dibiarkan dalam satu tingkat (*flat*). Harus ada pembagian segmen. Pencampuran server dan workstation dalam satu segmen rentan terhadap serangan penyadapan. Selain untuk keperluan keamanan, segmentasi juga dapat meningkatkan kinerja karena dapat mengurangi terjadinya *packet collision*. Jadi, server, *workstation*, dan perangkat-perangkat lain dipisahkan secara logik sesuai dengan segmennya. Jalur akses ke server kemudian dibatasi hanya untuk yang berhak saja.

Shared hub sebaiknya tidak digunakan lagi pada segmen yang ingin diamankan terhadap serangan penyadapan dan digantikan dengan switch, sebab *shared hub* membuka peluang adanya penyadapan.

Di dalam jaringan intranet sering digunakan protokol yang ti-

dak aman, seperti telnet, ftp, dan beberapa protokol yang dimulai dengan huruf “r” (seperti rlogin, rsh). Protokol ini menggunakan pasangan *userid* dan *password* dalam bentuk teks biasa sehingga mudah disadap. Jika jaringan Anda menggunakan protokol ini, gantikan dengan protokol yang lebih aman. Telnet dapat anda gantikan dengan ssh, sementara ftp dapat anda gantikan dengan scp. Ssh dan scp menggunakan enkripsi untuk komunikasinya sehingga lebih aman terhadap serangan penyadapan.


Kemudahan melakukan file sharing membuat orang lupa akan masalah keamanan yang ditimbulkannya. Sering dijumpai *workstation* yang memberikan akses baca tulis kepada direktori di *workstation*-nya. Kadang-kadang di direktori tersebut ditemukan berkas yang seharusnya hanya boleh diakses oleh kalangan terbatas. Akses tulis dapat digunakan oleh orang yang tidak berhak untuk menitipkan berkas. Jika berkas tersebut merupakan berkas yang *confidential*, pemilik workstation bisa mendapat masalah. Lebih jauh lagi,

file sharing ini bisa disusupi oleh virus atau trojan horse, baik secara manual (oleh pengguna yang nakal) atau secara otomatis oleh virus itu sendiri.

Mekanisme file sharing yang menggunakan port 139 ini sering

menjadi target serangan, khususnya pada sistem operasi MS Windows. Banyak contoh program eksploitasi yang ditujukan kepada port ini. Akibatnya komputer menjadi macet, *reboot*, atau bahkan memberikan akses shell (*command prompt*) yang dapat diakses dari jarak jauh. Untuk itu, sebaiknya mekanisme file sharing tidak diaktifkan jika tidak benar digunakan.

Teknologi wireless (WiFi) membuat permasalahan tersendiri di jaringan intranet. Access point untuk WiFi sudah demikian murah dan mudah dipasang sehingga kadang-kadang ada pengguna yang memasang perangkat tersebut tanpa izin dari pengelola jaringan, tanpa menyadari adanya potensi lubang keamanan. Access point sering kali “bocor” ke luar kantor sehingga dapat diakses orang yang tidak berhak.

Melihat permasalahan ini semua, pengelola jaringan tidak bisa menutup mata terhadap masalah keamanan intranet dengan beranggapan bahwa pengguna di dalam adalah orang baik-baik. Jaringan intranet harus diamankan secara sistematis. 



...sebaiknya mekanisme file sharing tidak diaktifkan jika tidak benar digunakan.