



Kejutan Virus di Awal Tahun

Awal tahun 2003 ini, tepatnya tanggal 24 Januari 2003, kita dikejutkan oleh virus yang mampu mematikan aktivitas jaringan Internet, *SQL Slammer*, yaitu sejenis virus yang menyerang program pengolah database, SQL dari Microsoft. Virus ini akan mempekerjakan CPU komputer menjadi 100% secara terus-menerus. Lalu, kalau kita sambung *Ethernet* dari komputer yang berisi virus ke *switch* atau *hub* jaringan yang ada, maka secara serentak seluruh jaringan tidak bisa bekerja, termasuk jaringan Internet-nya.

Sebetulnya, *patching* untuk virus *SQL Slammer* ini sudah ada bulan Juli tahun 2002. Hanya banyak pihak yang tidak begitu mengindahkan, karena sulitnya proses yang harus dilakukan, termasuk mengganti beberapa DLL secara manual. Pada kenyataannya *patch* yang dibuat enam bulan lalu itu, tidak mampu membendung serangan *SQL Slammer* yang pada akhir Januari 2003 yang lalu bekerja dengan serentak mematikan seluruh kegiatan jaringan Internet.

Kalau tahun lalu jaringan Internet diserang oleh *Code Red* melalui e-mail, maka sekarang giliran program Microsoft SQL yang diserang. Pada awalnya, diketahui bahwa virus *SQL Slammer* tidak merusak sistem operasi atau komputer secara langsung, yang pasti hanya akan mematikan kerjanya jaringan komputer atau Internet. Tetapi, setelah dilakukan beberapa penelitian sekitar virus ini, ternyata virus akan merusak data di komputer yang terserang, jika di dalamnya terpasang program komputer lain yang berhubungan atau merupakan *plug-in* dari Microsoft SQL, seperti yang dilaporkan oleh satu situs di Internet: <http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=10&tabid=13>.

Salah satu perusahaan yang menjadi korban pertama serangan virus *SQL Slammer*, yaitu tanggal 24 Januari tengah malam adalah *Bank of America*, di mana virus ini melumpuhkan 13.000 mesin ATM yang menggunakan TCP/IP sebagai protokol jaringannya. Kemudian perusahaan penerbangan *Continental Airlines* juga terhenti pelayanan *ticketing*-nya, karena jaringannya tidak bisa mengakses dan diakses.

Selain di Amerika, Korea Selatan yang merupakan negara pemakai terbesar jaringan Internet di Asia, juga mati total dalam beberapa jam. Kejadian ini juga berdampak pada beberapa ISP yang ada di Indonesia, sudah tentu yang menggunakan Microsoft SQL di jaringannya.

SQL Slammer adalah virus kecil, besarnya hanya 367 byte saja. Cara kerjanya, menyerang komputer dan sistem operasi melalui *port* 1434/UDP. Seperti kita ketahui, dalam jaringan Internet kita bisa menentukan banyak *port* untuk berbagai keperluan, dan *port* 1434 inilah yang diserang oleh *SQL Slammer* karena sebelumnya dipakai sebagai *backdoor* dari programmer-programmer SQL. Cara untuk menangani virus ini tidak terlalu rumit, cukup memperbarui programnya (*update* atau *patch* programnya) atau menginstalasi program Microsoft SQL yang baru. Di samping tersedianya beberapa *script* yang bisa dipakai untuk menghindari serangan melalui *port* 1433 tersebut.

Karena kejadian ini, beberapa pengguna program Microsoft SQL menyalahkan Microsoft, yang lalai melakukan perbaikan dan penutupan *port* yang dapat membahayakan program yang dijalankan di jaringan Internet (lihat *mailing list* <http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A1=ind0301&L=ntbugtraq>).

Fenomena ini akan selalu terjadi pada pemakaian peranti lunak komputer, karena biar bagaimanapun pola pikir manusia akan selalu bervariasi dan tidak ada batasnya—di atas langit masih ada langit.

Makanya, konsep Linux yang membuka semua programnya, bisa mengurangi risiko penyusupan yang tidak diketahui oleh banyak orang.

Berjangkitnya virus pada sistem program tertutup seperti yang dikembangkan Microsoft, tidak akan sering terjadi di dalam sistem terbuka yang dianut oleh Linux. Dan memang, dalam sepuluh tahun belakangan ini, kenyataan bahwa penyebaran virus di produk Microsoft relatif lebih mudah dan sering terjadi dibandingkan virus yang berjangkit di sistem operasi Linux. Sehingga muncul pula anggapan negatif, bahwa yang membuat virus adalah “orang dalam” yang memang mengetahui seluk beluk program yang dikembangkan, yang bisa saja bekerja sama dengan para pembuat antivirus untuk bisa mendapatkan bisnis dari seluruh kejadiannya.

Jadi, beruntung bagi kita yang menggunakan program dengan metoda *open source*—seperti Linux, di mana tidak ada yang lebih hebat dari yang lain, semua mengetahui dengan tepat apa yang kita lakukan. ☺

... yang membuat virus itu sendiri adalah “orang dalam” yang mengetahui seluk beluk program yang dikembangkan...