BAB V
PEMBAHASAN MASALAH



5.1. Cara Menangani Masalah

Virus dapat dicegah dengan cara sebagai berikut :

- Disket darurat untuk mencegah virus akut

Apakah disket Boot sudah diperbaharui? Disket ini berguna bila PC tidak lagi bekerja dengan baik. Yang harus dilakukan adalah memboot dari disket yang "bersih" dan memeriksa hardisk dengan program antivirus terbaru dari disket yang telah diproteksi. Bila antivirus dijalankan dari system yang terinfeksi, dapat mengakibatkan penyebaran virus ke berbagai file pada hardisk.

Buatlah disket darurat (dengan proteksi). Bila tidak, windows atau software antivirus juga membantu membuatnya: Pada Windows 9x jalankan prosesnya melalui "Start|Setting|Control Panel|Add/Remove Programs". Lalu pilih "Startup Disk|Create Disk...."[6]. Selanjutnya Windows akan membuat disket darurat bagi anda.

Bila anda ingin mengakses CD-ROM drive nantinya, copy driver CD-ROM drive dan MSCDEX.EXE dari sub direktori COMMAND disket. Masukan driver ke dalam file CONFIG.SYS, dan pada file AUTOEXEC.BAT cantumkan file MSCDEX.EXE.

Pada Windows NT, disket boot dibuat dengan menjalankan file WINNT32.EXE dalam direktori i386 Windows NT-CD dengan parameter "ox/".

Norton Antivirus, seperti halnya scanner anti virus lainnya juga membuat disket darurat/boot. Norton Antivirus selanjutnya akan membuat 3 disket darurat: Yang pertama untuk proses boot (tanpa driver CD), yang lainnya berisi virus scanner.

- Jangan beri kesempatan virus boot untuk merusak

Jenis virus boot selalu berada dalam daftar TopTen virus terpopuler. Sebuah trik sederhana dapat digunakan untuk mengusir virus tersebut secara permanen. Tentukan prioritas boot dalam BIOS setup. Prioritas pertama pilih harddisk, lalu drive disket atau CD-ROM drive, misalnya dengan urutan "C:,A,CD-ROM". Tanpa biaya dan tanpa efek samping. Mulai kini Anda tak akan diganggu oleh virus boot. Bila sewaktu-waktu harus mem-boot dari disket, Anda tinggal merubah urutan boot pada BIOS setup.

- Buat penghalang bagi virus macro

Dalam Office 2000 fasilitas macro pada Word, Excel, Powerpoint, Outlook, dan Frontpage tidak disediakan bila tingkat keamanan diatur "High". Pada word bahkan diatur sebagai setting default (standar). Sangat ideal bagi pemakai biasa yang tidak menggunakan dan menulis fasilitas macro. Hanya macro bersetifikat yang bebas dari tingkat keamanan. Bila ingin menguji macro buatan sendiri, turunkan tingkat keamanan ke "middle". Maka saat membuka dokumen, seperti halnya pada Office 97, maka pilihan yang ada adalah mengaktifkan macro atau tidak.

- Perbaiki Outlook: Melindungi serangan Trojan Horse

Bila Trojan Horse menyusup lewat lampiran e-mail, klik ganda pada program tersebut akan mengaktifkannya. Microsoft mengantisipasinya dengan membuat update untuk Outlook 97, 98 dan 2000 sehingga Outlook tidak hanya memberi peringatan akan bahaya Trojan Horse, melainkan juga menyimpan semua file EXE, COM dan BAT. Ini mencegah menjalankan aplikasi yang terlampir pada e-mail yang datang. Sebuah Patch untuk Outlook besarnya 2-3 Mb, tak dapat dibatalkan dan merupakan pengganti antivirus. Patch tersebut dapat anda download pada : http://officeupdate.microsoft.com/welcome/outlook.asp.

- Hati-hati terhadap program tak dikenal

Program atau dokumen yang didownload dari Internet, ataupun mungkin bermain di halaman web milik hacker dapat membahayakan. bila PCnya tiba-tiba berlaku aneh. Waspadai dokumen dan terutama program dari sumber tak dikenal. Bila perlu, periksa segera setelah didownload, apakah ada virusnya.

- Buat backup pengaman untuk berjaga-jaga

Pengamanan data secara teratur memang bukan penangkal virus, tapi bermanfaat untuk menghindari akibat infeksi yang tidak menyenangkan, misalnya kehilangan data. Backup-lah setiap selesai bekerja semua file baru atau yang baru diubah dalam sebuah disket atau media backup lainnya. Program backup Windows cukup handal melacak file yang baru diubah.

- Aktifkan pengaman virus macro

Idealnya program antivirus berguna untuk menyingkirkan virus, tapi ia juga memungkinkan terjadinya infeksi yang kedua kalinya. Soalnya virus macro yang modern mampu melewati pengaman virus Office 97 dan membuatnya non-aktif. Setelah desinfeksi, Word lebih rentan lagi tehadap virus. Versi yang tidak terlalu canggih pun bisa menyusup. Setelah kasus virus pada Word, pastikan pengaman virus aktif.

- Hanya bila terpaksa: Format ulang harddisk

Setelah harrdisk terkena virus biasanya kita berfikir: Harrdisk yang terkena virus harus di format ulang , adapun cara suapaya harrdisk tersebut tidak di format

yaitu Pertama, Virus boot seperti Parity_Boot yang menduduki MBR, tak terganggu oleh format ulang. Kedua, biasanya tindakan yang terencana sudah mencukupi, yaitu dengan memakai antivirus.

Bila program antivirus tak berdaya membersihkan program atau dokumen, instalasi ulang programnya dan gunakan data backup. Kalau sistem masih belum tertolong atau tidak stabil akibat kerusakan system file, baru terpaksa hardisk diformat ulang. Sebelumnya selamatkan dulu semua data!.

- Singkirkan file Word yang rusak dari harddisk

Bila dokumen tak dapat dibersihkan dengan antivirus, hapus atau isolasikan pada disket. Tandai disket tersebut dengan "terinfeksi". Selanjutnya bersihkan dengan scanner lain atau tanyakan pada perusahaan antivirus. Yang penting singkirkan dokumen terinfeksi dari harddisk.

Awas: Mengubah nama file sama sekali tak berguna. Bila diklik ganda, Windows langsung mengenali struktur internalnya, misal file Word, dan membukanya langsung dengan aplikasi tersebut.

Penanganan Virus yang telah di lakukan oleh PT.Pertamina UP VI Balongan

1. Memasang Firewall pada pintu masuk Internet dengan Cisco PIX 505, Pada konfigurasi PIX di set agar port tertentu yang hanya boleh lewat, jika ada port-port yang lain ataupun yang dianggap mencurigakan port tersebut di blok agar tidak dapat masuk melalui Internet.
2. Memasang Anti Virus Server, dengan Symantec Norton Anti Virus versi 9.0, dan secara rutin 1-2 hari virus definition di update.
3. Memasang Norton Anti Virus yang sama persis dengan servernya di semua PC Client, kurang lebih ada 500 PC yang ada di PT. Pertamina UP VI Balongan yang sudah di pasang Norton Anti Virus.
4. Memberi Penerangan atau Sosialisasi terhadap user pemakai PC tentang bahaya Virus termasuk agar hati-hati terhadap Email Asing.

5. Memasang Anti Virus di Email Server Trand Macro for Exchange.
6. Menyeragamkan System Operasi yang dipakai dengan Linux yang kemungkinan kecil Virus tidak dapat menyebar. Kalaupun Linux tidak dipakai dan System Operasinya menggunakan berbagai macam Windows maka setiap PC harus memiliki Norton Anti Virus yang sama dengan Servernya, ataupun mempublikasikan bahaya Virus terhadap PC.
7. Membatasi akses dari jaringan internal ke internet atau sebaliknya. Yang mampu mengurangi Virus yang masuk ke dalam.

5.2. Pembahasan / Analisa Masalah

Pada bulan November 1988, Worm Morris telah memblokir ribuan komputer berbasis Unix di Internet. Adapun pada komputer basis windows, ancaman ini baru timbul setelah banyak pemakai menggunakan e-mail di jaringan ataupun Internet. Contoh yang terbaru adalah Worm Explore-Zip, yang pada akhir Juni lalu sempat menimbulkan kepanikan pada masyarakat Internet. Sebagai file lampiran e-mail yang menyerupai self-extracting ZIP (karena memiliki icon program Winzip), dengan mudah ia dapat menyebarkan diri. Hal itu disebabkan karena pemakai tidak curiga akan langsung mengekstrak file tersebut untuk menjalankannya.

Penyebaran software berbahaya ala Worm memberikan tantangan baru bagi industri software antivirus. Program mereka harus mampu "mematikan" Worm sebelum menyebar secara luas lewat e-mail. Persoalannya adalah jika Worm tersebut dianalisa dan update antivirus penangkalnya selesai dibuat, maka dirasakan waktu yang dibutuhkan terlalu lama. Sementara itu, lampiran e-mail yang berbahaya terus berdatangan sehingga dapat membuat sebuah perusahaan kehilangan kontak dengan dunia luar. Beberapa perusahaan mengantisipasinya dengan menghilangkan semua lampiran yang tak dikenal dan dicurigai berbahaya dengan membuat Firewall.

Tidak semua pemakai komputer berlindung di balik Firewall, terutama pemakai pribadi, yang semakin sering berhadapan dengan program sejenis Trojan Horse, seperti backdoor. Secara diam-diam backdoor membuka PC anda ke Internet bila sedang online, sehingga dari sudut manapun di dunia, tampilan monitor PC anda

dapat dilihat baik data, e-mail, atau password. Beberapa tipe backdoor mengumpulkan password ketika anda offline, lalu mengirimkannya ke internet ketika online. Jika itu semua terjadi, maka tidak sulit bagi orang yang mengintai untuk mengcopy atau menghapus file pada PC anda.

Internet membuka peluang bagi aktivitas yang merusak, Prinsip lama "Virus yang agresif mudah dikenali sehingga tidak dapat berkembang lebih jauh" tak dapat dipertahankan lagi. Terbukti dengan adanya worm perusak Explore-Zip yang telah menulari PC lain via e-mail. Pemakai PC baru menyadari keberadaan worm ini setelah file-file pada PC-nya rusak (ukurannya menjadi 0 byte).

Pembuat virus bukan lagi seorang anak ingusan, Dari golongan mana saja pembuat virus atau Trojan Horse yang menyebabkan kerugian pada orang lain tersebut? Dapat dikatakan hampir semuanya laki-laki. Hingga kini perempuan hanya dikenal sebagai simpatisan kelompok pembuat virus saja. Sebelumnya para pembuat virus kebanyakan berasal dari kalangan pelajar atau mahasiswa yang belum "matang". Contohnya, mahasiswa informatik Taiwan, Cheng Ing-Hau, yang menyebabkan ribuan PC tidak dapat digunakan di seluruh dunia. Ia berusia 23 tahun saat menyebarkan virus CIH (berasal dari nama inisialnya) yang merusak Flash BIOS pada PC.

"Banyak pembuat virus yang cuma ingin menunjukan kepintarannya", demikian menurut Paul Ducklin, kepala bagian pengembangan Sophos, perusahaan antivirus di Inggris. "Mereka tak punya cara lain untuk menyombongkan diri." Namun Paul tak melihat prospek karir yang baik bagi mereka: "Yang mampu melempar batu belum tentu tukang batu yang baik.", demikian ia melukiskannya.

Pembuat virus gemar membuat trik-trik dan memanfaatkan perintah atau feature yang tidak sempurna pada beberapa software. Dilain pihak pembuat antivirus harus membuat program handal yang dapat dijalankan pada berbagai system operasi. Bila sebuah virus tidak melancarkan fungsi perusak serta menyebarkan diri pada semua komputer, maka tak akan ada yang merasa terganggu. Sebaliknya bila antivirus gagal berfungsi, pelanggan langsung mengeluh.

Dengan adanya 500-800 virus baru yang muncul setiap bulan, sepertinya sulit diimbangi. "Sekitar 7 dari 10 virus sangat sulit disingkirkan"[5], Tak heran bila perusahaan software memperkuat diri dengan melakukan akuisisi. Dapat disebutkan disini seperti NAI (Network Associates), pembuat software McAfee, menelan pesaingnya Dr. Solomon's. Symantec, Norton Antivirus, pembuat antivirus kedua terbesar, mengambil alih antivirus IBM. Perusahaan Norwegia, "Norman Data Defense" membeli antivirus "Thunderbyte" dari Belanda.