

Keamanan dan Etika dalam Teknologi Informasi

Keamanan

- Keamanan komputer memiliki beberapa ancaman:
 - Serangan melalui Internet dan Jaringan
 - Malware (Malicious Ware)
 - Serangan denial of Service (DOS Attack)
 - Back Door
 - Spoofing
 - Penggunaan tak terotorisasi
 - Pencurian Pencurian Hardware dan Software
 - Pencurian Informasi

- Serangan melalui Internet dan Jaringan dibagi menjadi 3, yaitu
 - Malware (Malicious Ware)
 - Serangan denial of Service (DOS Attack)
 - Akses dan penggunaan tak terotorisasi

Serangan melalui Internet dan Jaringan

- **Malware**
 - Virus : program yang bertujuan untuk mengubah cara bekerja komputer tanpa seizin pengguna.
 - Worm : program yang menggandakan dirinya secara berulang-ulang di komputer sehingga menghabiskan sumber daya.
 - Trojan : program/sesuatu yang menyerupai program yang bersembunyi di dalam komputer kita
 - ➔ Malware ini akan mengirimkan payload (kejadian destruktif yang dikirimkan oleh program)
- Malware ini dapat diatasi menggunakan program Antivirus

- DOS Attack
 - Serangan yg bertujuan untuk mengganggu akses komputer pada layanan Web atau email.
 - Pelaku akan mengirimkan data yang tak bermanfaat secara berulang-ulang.
 - Akibatnya jaringan akan memblok pengunjung lainnya
- Back Door
 - Program yg memungkinkan pengguna tak terotosasi untuk masuk ke komputer tertentu
- Spoofing
 - Teknik untuk memalsukan IP komputer sehingga dipercaya oleh jaringan
- Serangan ini dapat dilindungi oleh firewall

Penggunaan Tak Terotorisasi

- Penggunaan tak terotorisasi: penggunaan komputer/data-data di dalamnya untuk aktivitas ilegal atau tanpa persetujuan pengguna.
- Masalah ini dapat diselesaikan dengan menggunakan metode kontrol akses
 - Kontrol akses : tindakan keamanan yang menentukan siapa, kapan dan tindakan apa yang dapat diambil oleh seseorang terhadap sistem
 - Contohnya: penggunaan login&password dan perangkat biometrik

Pencurian Hardware & Software

- Pencurian hardware: diambilnya hardware dari lokasi tertentu dapat diatasi dengan memberikan kunci, gembok dsb.
- Pencurian software: seseorang mencuri media piranti lunak dan dengan sengaja menghapus program atau secara ilegal menyalin program
- Termasuk dalam kategori pencurian software adalah pembajakan.

Pencurian Informasi

- Terjadi ketika seseorang mencuri informasi pribadi atau yang sifatnya rahasia
- Untuk melindungi pencurian informasi ini menggunakan metode enkripsi
- Enkripsi: mengubah karakter yang dapat dibaca menjadi tidak dapat dibaca
 - Salah satu isu terpenting saat ini dalam e-gov adalah tanda tangan digital
 - Sertifikat digital sering digunakan untuk transaksi online

Etika Komputer

- Untuk mengatasi berbagai pencurian di atas diperlukan etika komputer
- Adalah panduan moral yang mengatur penggunaan komputer dan sistem informasi

Kejahatan cyber

- Ada berbagai kejahatan cyber yang terjadi
 - Hacker: seseorang yg mengakses komputer/jaringan secara ilegal
 - Cracker: seseorang yg mengakses komputer/jaringan secara ilegal dan memiliki niat buruk
 - Script kiddie: serupa dengan cracker tapi tidak memiliki keahlian teknis
 - Cyberterrorist: seseorang yang menggunakan Internet atau jaringan untuk merusak dan menghancurkan komputer/jaringan dengan alasan politis

- Phishing/Pharming: trik yang dilakukan pelaku kejahatan untuk mendapatkan informasi rahasia, jika phishing menggunakan email, pharming langsung menuju ke web tertentu.
- Spam: email yang tidak diinginkan yang dikirim ke banyak penerima sekaligus
- Spyware: program yang secara tidak sengaja terpasang untuk mengirimkan informasi pengguna kepada pihak lain salah satu bentuknya adalah adware

Isu terkini di Indonesia

- UU ITE (Undang-undang Informasi dan Transaksi Elektronik) sudah disahkan menjadi UU dengan nomor 11/2008. UU ini antara lain mengatur
 - Pornografi di Internet
 - Transaksi elektronik
 - Etika penggunaan Internet
- Munculnya e-Announcement sebagai cikal bakal e-Procurement
 - E-Procurement mampu mengurangi kerugian negara akibat penyelewengan dalam pengadaan barang&jasa
- Adanya blue print sisfonas semenjak 2002