Pengantar Teknologi Informasi

12 KEAMANAN KOMPUTER

KEAMANAN KOMPUTER

Penyebab munculnya Kejahatan komputer:

- Aplikasi bisnis yang menggunakan teknologi komputer dan jaringan komputer semakin meningkat.
- Server terdesentralisasi dan terdistribusi menyebabkan lebih banyak sistem yang harus ditangani.
- Transisi dari vendor tunggal ke multi vendor sehingga lebih banyak sistem atau perangkat yang harus dimengerti dan masalah *interoperability* antar vendor yang lebih sulit ditangani.
- Meningkatnya kemampuan pemakai di bidang komputer.
- Mudah diperolehnya software untuk menyerang komputer dan jaringan komputer.
- Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.
- Semakin kompleksnya sistem yang digunakan.
- Terjadinya lubang keamanan yang disebabkan oleh kesalahan program (bugs).
- Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global.

Aspek Keamanan

- ***Authentication***, yaitu agar penerima informasi dapat memastikan tersebut datang dari orang yang dimintai informasi.
- ***Integrity***, yaitu keaslian pesan yang dikirim melalui jaringan.
- ***Nonrepudiation***, hal yang bersangkutan dengan pengirim.
- ***Authority***, informasi yang berada dijaringan tidak dapat dimodifikasi.
- ***Confidentiality***, usaha untuk menjaga informasi.
- ***Privacy***, lebih ke arah data.
- ***Availability***, aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- ***Access control***, cara pengaturan akses ke informasi.

Tujuan / Syarat Keamanan

- **Kerahasiaan (*secrecy*)**; berhubungan dengan hak akses untuk membaca data atau informasi dari suatu sistem komputer.
- **Integritas (*integrity*)**; berhubungan dengan hak akses untuk mengubah data atau informasi dalam sistem komputer.
- **Ketersediaan (*availability*)**; berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan.

Lingkup Pengamanan

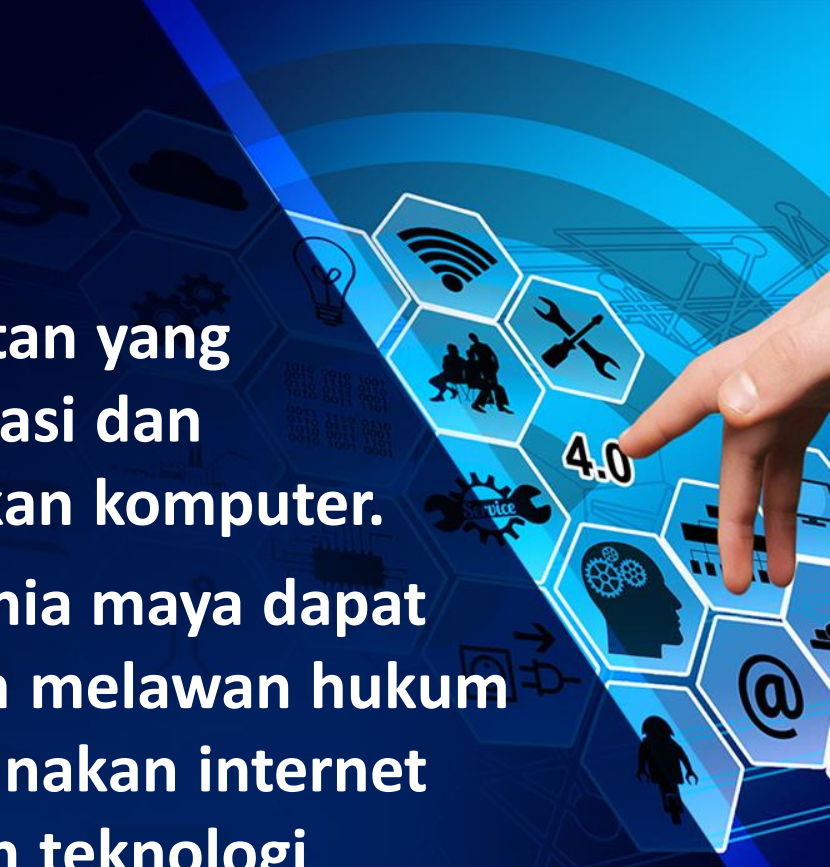
- Pengamanan secara fisik (lokasi).
- Pengamanan akses (log on user).
- Pengamanan data (hak akses user).
- Pengamanan komunikasi jaringan (kriptografi).

Bentuk –bentuk Ancaman (Threats)

- **Interupsi (*interuption*)**; bentuk ancaman terhadap ketersediaan dimana data dirusak sehingga tidak dapat digunakan lagi, baik fisik maupun non fisik.
- **Intersepsi (*interception*)**; bentuk ancaman terhadap secrecy dimana pihak yang tidak berhak mendapat hak akses untuk membaca data atau informasi dari sistem komputer.
- **Modifikasi (*modification*)**; bentuk ancaman terhadap integritas dimana pihak yang tidak berhak mendapat hak akses untuk mengubah data atau informasi dari sistem komputer.
- **Pabrikasi (*fabrication*)**; bentuk ancaman terhadap integritas dimana tindakannya adalah dengan memasukkan meniru atau memasukkan objek lain ke dalam sistem komputer.

Cyber Crime

- ***Cyber crime*** **merupakan kejahatan yang menggunakan teknologi informasi dan komunikasi dengan menggunakan komputer.**
- ***Cyber crime*** **atau kejahatan dunia maya dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan komunikasi.**



Karakter Cyber Crime

- Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis yang terjadi di ruang/wilayah maya (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
- Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan jaringan telekomunikasi atau internet.
- Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional.
- Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
- Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

Celah Keamanan

Menurut David Icove, celah keamanan dapat diklasifikasikan menjadi empat, yaitu:

- keamanan bersifat fisik (physical security); termasuk akses orang, media, dan peralatan yang digunakan.
- Keamanan yang berhubungan dengan orang (personel); termasuk identifikasi dan profil resiko dari orang yang memiliki akses.
- Keamanan dari data dan media serta teknik komunikasi; Kelemahan dari software yang digunakan untuk mengolah data.
- Keamanan dalam operasi; prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan.

Hacker dan Cracker

Hacker adalah istilah untuk seseorang yang mempelajari, memodifikasi, menganalisa dan masuk ke sebuah jaringan komputer

Cracker adalah seseorang yang masuk ke sistem orang lain dengan sengaja melawan keamanan komputer untuk maksud / tujuan jahat.

Hacker **menurut Eric Raymond** ada 5 karakteristik:

1. seorang yang suka belajar detail dari bahasa pemrograman atau sistem.
2. seorang yang melakukan pemrograman, bukan hanya teori.
3. seorang yang menghargai, menikmati hasil hacking orang lain.
4. seorang yang secara cepat dapat belajar pemrograman.
5. seorang yang ahli dalam bahasa pemrograman atau sistem tertentu.

Jenis – Jenis Cybercrime

1. Carding
2. Cracking
3. Joy computing
4. Hacking
5. The trojan horse
6. Data leakage
7. Data diddling
8. To frustate data communication
9. Software piracy
10. Cyber Espionage
11. Infringements of Privacy
12. Data Forgery
13. Unauthorized Access to Computer System and Service
14. Cyber Sabotage and Extortion
15. Offense against Intellectual Property
16. Illegal Contents

Program Pengganggu / Perusak

Bug

Bug merupakan kesalahan-kesalahan yang terdapat pada suatu program aplikasi yang terjadi/ tercipta secara tidak disengaja. Hal ini umumnya dikarenakan kecerobohan/ keteledoran dari pihak programer pada waktu menulis program tersebut. Bug ini mempunyai dampak yang bermacam-macam seperti komputer menjadi hang atau bahkan bisa merusak media penyinpanan pada sistem komputer milik Anda.

Program Pengganggu / Perusak

Chameleons

Chameleons sesuai dengan namanya merupakan program yang diselundupkan/ disisipkan ke dalam suatu sistem komputer dan berfungsi untuk mencuri data/ informasi dari sistem komputer yang bersangkutan. Program ini tidak merusak peralatan pada sistem komputer yang dijangkitinya, targetnya ialah mendapatkan data dan kadang kala berusaha untuk melakukan pengubahan pada data tersebut.

Program Pengganggu / Perusak

Logic Bomb

Bomb ini akan ditempatkan/ dikirimkan secara diam-diam pada suatu sistem komputer yang menjadi target dan akan meledak bila pemicunya diaktifkan. Berdasarkan pemicu yang digunakan, Logic bomb dapat digolongkan menjadi tiga, yaitu software bomb, logic/condition bomb, time bomb. Software bomb akan meledak jika dipicu oleh suatu software tertentu, Logic/condition bomb akan meledak jika memenuhi suatu kondisi tertentu, sedangkan time bomb akan meledak pada waktu yang telah ditentukan. Logic Bomb merupakan program yang dimasukkan ke dalam suatu komputer yang bekerja untuk memeriksa kumpulan kondisi di dalam suatu sistem. Jika kondisi yang dimaksud terpenuhi, maka program akan mengeksekusi perintah yang ada di dalamnya. Program ini berjalan jika ada pemicu. Biasanya pemicunya adalah jika user menjalankan program tertentu atau menekan salah satu tombol keyboard.

Trojan Horse

Trojan atau trojan Horse sengaja dibuat dengan tujuan yang jahat. Trojan tidak dapat memproduksi dirinya sendiri, biasanya dibawa oleh suatu program utility lain. program tersebut mengandung trojan dan trojan itu “bergaya” seolah-olah suatu program tersebut. Trojan ini tidak berbahaya sampai dilakukan eksekusi pada program. tetapi biasanya trojan ini tersembunyi dari aplikasi utama sehingga user secara tidak sengaja akan membuka program yang sebenarnya adalah trojan. Aktivitas dari trojan biasanya menghapus file, mengcapture password, dan sebagainya. Trojan dapat dibedakan menjadi dua yaitu DOS Trojan (berjalan under DOS, mengurangi kecepatan komputer dan menghapus file) dan Windows Trojan (berjalan di Mic. Windows). Contoh Trojan Horse: Win-Trojan / Back Orifice, Win-Trojan / SubSeven, Win-Trojan / Ecokys.

Virus

Program yang dapat mengcopy dirinya sendiri dan menginfeksi komputer tanpa sepengetahuan dari user. Virus terdiri dari kumpulan kode yang dapat memodifikasi target kode yang sedang berjalan, atau dapat pula memodifikasi struktur internal target kode, sehingga target kode tidak dapat berjalan. Virus kadang menampilkan pesan yang tidak kita sukai, merusak tampilan, merusak data dan sebagainya. Virus masih dapat diklasifikasikan menjadi Boot Virus (virus yang berada di boot sector, muncul ketika komputer dinyalakan), File virus (virus yang menginfeksi program exe), Multipart virus (menyerang boot sector dan file), dan Macro virus (menyerang dan menginfeksi office document). Contoh virus: Brain, Ohe half, Die hard, XM/Laroux, Win95/CIH .

Worm

Worm merupakan suatu program pengganggu yang dapat memperbanyak diri dan akan selalu berusaha menyebarkan diri dari satu komputer ke komputer yang lain dalam suatu jaringan. Worm menjadikan ukuran suatu file menjadi membengkak dan bahkan dapat menguras kapasitas dari media penyimanan. Contoh worm: I-Worm/Happy99(Ska), I-Worm/ExploreZIP, I-Worm/PrettyPark, I-Worm/MyPics.

Sejarah Perkembangan Cyber Crime di Indonesia

Pada Tahun 1982

- Telah terjadi penggelapan uang di bank melalui komputer sebagaimana diberitakan "Suara Pembaharuan" edisi 10 Januari 1991 tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372.100.000,00 dengan menggunakan sarana komputer.

Pada Tahun 2003

- Carding salah satu jenis cyber crime yang terjadi di Bandungsekitar Tahun 2003. Carding me rupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang laindan digunakan dalam transaksi perdagangan di internet.

Pada Tahun 2009

- Penyebaran virus dengan sengaja, ini adalah salah satu jenis kasus cyber crime yang terjadi pada bulan Juli 2009, infeksi modifikasi New Koobface, worm yang mampu membajak akun Twitter dan menular melalui postingannya, dan menjangkiti semua follower.

Pada Tahun 2016

- Pembajakan papan Billboard Videotron tanggal 20 september 2016 di Jalan Prapanca Raya, Kebayoran Baru, Jakarta Selatan sekira pukul 13.00 WIB. Yang dilakukan oleh orang yang tidak bertanggung jawab.

Pada Tahun 2017

- Pada bulan Mei 2017 terdapat isu bahwa kita tidak boleh menyambungkan perangkat elektronik atau gadget kita ke internet Karena terancam akan kehilangan data pribadi kita dan bila ingin dikembalikan harus menyerahkan sejumlah uang tebusan yang nilainya tidak sedikit, dan disebut sebut disebabkan oleh virus "Wannacry" yang membuat gaduh netizen dunia

Upaya pencegahan Cybercrime

1. Personal

Ada beberapa hal yang dapat dilakukan untuk mengatasi cyber crime secara personal, antara lain :

a. Internet Firewall.
b. Kriptografi (Seni menyandikan data).
c. Secure Socket Layer.
d. Menutup service yang tidak digunakan.
e. Adanya sistem pemantau serangan.
f. Melakukan back up secara rutin.
g. Adanya pemantau integritas sistem.

2. Pemerintahan

Upaya yang harus dilakukan pemerintah untuk mencegah meningkat nya kasus cyber crime:

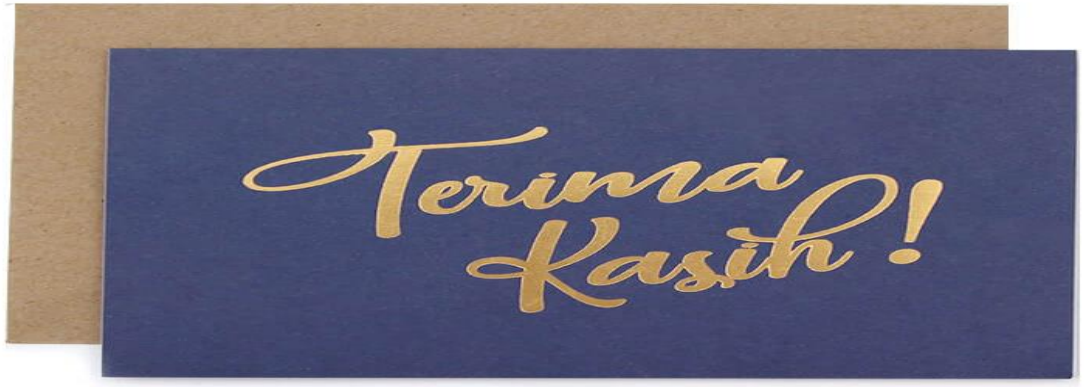
a. Meningkatkan modernisasi hukum pidana nasional beserta hukum acaranya.
b. Meningkatkan sistem pengamanan jaringan komputer nasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum
d. Meningkatkan kesadaran masyarakat mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
e. Membentuk badan penyelidik internet.

Cara Mengantisipasi Cybercrime

Pengamanan Internet

- Melindungi Komputer
- Melindungi Identitas
- Selalu Up to Date
- Amankan E-mail
- Melindungi Account
- dll


Service


Terima
Kasih!