KEJAHATAN BIDANG TEKNOLOGI INFORMASI

Pendahuluan

- Kecenderungan insiden di bidang teknologi komputer dan komunikasi digolongkan ke dalam prgram hacking :
  - Packet flooding
  - Packet sniffing
  - Backdoor
- Secara umum kita fokus pada sistem komputer berbasis windows
- Dalam kenyataan kejahatan komputer sudah sangat meluas, sudah tidak melihat kepada basis sistem operasi saja.

KEJAHATAN BIDANG TEKNOLOGI INFORMASI

- Beberapa istilah Kejahatan di bidang Teknologi Informasi :
  - Cybercrime
  - Kejahatan Mayantara (Barda Nawawi A.)
  - Computer Crime
  - Computer Abuse
  - Computer Fraud
  - Computer Related Crime dll

- ***Computer Crime*** ➔ perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.
- ***Cybercrime*** ➔ perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi (Teguh Wahyono, S. Kom, 2006)

Karakteristik unik Kejahatan bidang TI :

- **Ruang Lingkup kejahatan**
  - Bersifat global (melintasi batas negara) menyebabkan sulit menentukan yuridiksi hukum negara mana yang berlaku terhadapnya.
- **Sifat Kejahatan**
  - Tidak menimbulkan kekacauan yang mudah terlihat (non-violence), sehingga ketakutan terhadap kejahatan tersebut tidak mudah timbul.
- **Pelaku Kejahatan**
  - Pelaku kejahatan ini tidak mudah didentifikasi, namun memiliki ciri khusus yaitu pelakunya menguasai penggunaan internet / komputer.
- **Modus Kejahatan**
  - Modus kejahatan hanya dapat dimengerti oleh orang yang mengerti dan menguasai bidang teknologi informasi.
- **Jenis Kerugian**
  - Kerugian yang ditimbulkan lebih luas, termasuk kerugian dibidang politik, ekonomi, sosial dan budaya.

Kejahatan Bidang TI

- Menurut Heru Sutadi, 2003 digolongkan menjadi dua bagian, yaitu :
  - Kejahatan yang menggunakan TI sebagai **FASILITAS**
    - Contoh : pembajakan, pornografi, pemalsuan dan pencurian kartu kredit, penipuan lewat e-mail, penipuan dan pembobolan rekening bank, perjudian online, terorisme, situs sesat, Isu SARA dll
  - Kejahatan yang menjadikan sistem dan fasilitas TI sebagai **SASARAN.**
    - Contoh : pencurian data pribadi, pembuatan dan penyebaran virus komputer, pembobolan situs, cyberwar dll

JENIS CYBERCRIME

- Menurut Teguh Wahyono, S. Kom., 2006 jenis cybercrime dikelompokan dalam :
  1. Cybercrime berdasarkan JENIS AKTIFITAS
  2. Cybercrime berdasarkan MOTIF KEGIATAN
  3. Cybercrime berdasarkan SASARAN KEJAHATAN

CYBERCRIME ; JENIS AKTIFITAS

a. Unauthorized Acces

- Kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer sedara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya, contoh : Probing dan Port Scanning

b. Illegal Contents

- Kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum, contoh : penyebarluasan pornografi, isu-isu / fitnah terhadap individu (biasanya public figure).

CYBERCRIME ; JENIS AKTIFITAS

c. Penyebaran virus secara sengaja

- Melakukan penyebaran virus yang merugikan seseorang atau institusi dengan sengaja

d. Data Forgery

- Kejahatan yang dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet, biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

e. Cyber Espionage, Sabotage and Extortion

- *Cyber Espionage* merupakan kejahatan yang memanfaaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.
- *Sabotage* and *Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

CYBERCRIME ; JENIS AKTIFITAS

f. Cyberstalking

- Kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan melakukan teror melalui pengiriman e-mail secara berulang-ulang tanpa disertai identitas yang jelas.

g. Carding

- Kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

h. Hacking dan Cracking

- Hacker sebenarnya memiliki konotasi yang netral, namun bila kemampuan penguasaan sistem komputer yang tinggi dari seorang hacker ini disalah-gunakan untuk hal negatif, misalnya dengan melakukan perusakan di internet maka hacker ini disebut sebagai cracker. Aktifitas cracking di internet meliputi pembajakan account milik orang lain, pembajakan situs web, probing, penyebaran virus, hingga pelumpuhan target sasaran (menyebabkan hang, crash).

CYBERCRIME ; JENIS AKTIFITAS

i. Cybersquatting and Typosquatting

- *Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis.
- *Typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain, biasanya merupakan nama domain saingan perusahaan.

j. Hijacking

- Hijacking merupakan kejahatan pembajakan terhadap hasil karya orang lain, biasanya pembajakan perangkat lunak (Software Piracy).

k. Cyber Terorism

- Kejahatan yang dilakukan untuk mengancam pemerintah atau warga negara, termasuk cracking ke situs pemerintah atau militer.

CYBERCRIME ; JENIS KEGIATAN

a. Cybercrime sebagai tindakan murni kriminal

- Kejahatan ini murni motifnya kriminal, ada kesengajaan melakukan kejahatan, misalnya *carding* yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam bertransaksi di internet.

b. Cybercrime sebagai kejahatan "abu-abu"

- Perbuatan yang dilakukan dalam jenis ini masuk dalam "wilayah abu-abu", karena sulit untuk menentukan apakah hal tersebut merupakan kriminal atau bukan mengingat motif kegiatannya terkadang tidak dimaksudkan untuk berbuat kejahatan, misalnya *Probing* atau *portscanning* yaitu tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak mungkin, namun data yang diperoleh berpotensi untuk dilakukannya kejahatan.

CYBERCRIME ; JENIS KEJAHATAN

a. *Cybercrime yang menyerang **individu (Against Person)***
   - Jenis kejahatan ini sasaran serangannya adalah perorangan / individu yang memiliki sifat atau kriteria tertentu sesuai tujan penyerangan tersebut, contoh : Pornografi, Cyberstalking, Cyber-Tresspass.

b. *Cybercrime menyerang **Hak Milik (Against Property)***
   - Kejahatan yang dilakukan untuk mengganggu atau menyerang hak milik orang lain, contoh : pengaksesan komputer secara tidak sah, pencurian informasi, carding, cybersquatting, typosquatting, hijacking, data forgery.

c. *Cybercrime Menyerang **Pemerintah (Against Government)***
   - Kejahatan ini dilakukan dengan tujuan khusus penyerangan terhadap pemerintah, contoh : cyber terorism, craking ke situs resmi pemerintah.

PENANGGULANGAN CYBERCRIME

1. Pengamanan Sistem

- Tujuan yang paling nyata dari suatu sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sitem ini harus terintegrasi pada keseluruhan subsistem untuk mempersempit atau bahkan menutup adanya celah-celah unauthorised actions yang merugikan.

2. Penanggulangan Global

- OECD (The Organization for Economic Cooperation and Development) telah merekomendasikan beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan Cybercrime, sbb :

PENANGGULANGAN CYBERCRIME

3. Perlunya Cyberlaw

- Cybercrime belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.

4. Perlunya Dukungan Lembaga Khusus

- Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.
- Indonesia sendiri sudah memiliki IDCERT (Indonesia Computer Emergency Response Team) yang diperlukan bagi orang-orang untuk melaporkan masalah-masalah keamanan komputer,

Penanggulangan Global

1. Melakukan modernisasi hukum pidana nasional dengan hukum acaranya, yang diselaraskan dengan konvensi internasional.
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan cybercrime.
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.

Terima kasih