Cyber Crime

(Kejahatan di Dunia Maya)

Pembicara: **Hendi Hendratman ST**
Penulis buku-buku bidang Desain Grafis, Animasi & Multimedia
www.hendihen.com

1. SEKILAS CYBER CRIME

Latar Belakang

"Kasus cyber crime di Indonesia adalah nomor satu di dunia," *(Brigjen Anton Taba, Staf Ahli Kapolri)*

Definisi Cyber Crime

- Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet.
- Perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Jenis Cyber Crime

- Penggandaan Kartu (**Carding**)**.** Ex: *Skimming ATM,* Pencurian nomor Kartu kredit.
- Nama Domain **(Domain Name):** calo / *cybersquat*, plesetan / *typosquating* nama domain, nama pesaing
- Pembajakan / menggunakan komputer orang lain tanpa izin **(Hijacking)**
- Akses data tanpa izin **(Hacking),** bisa dengan virus atau cara lain
- Membocorkan data **(Data Leakage)**, terutama data rahasia negara / perusahaan.
- Pembajakan software **(Software piracy)** terhadap hak cipta yang dilindungi HAKI
- **Hoax**: pembuatan dan penyebaran berita palsu
- Dll

Contoh Kasus Cyber Crime di Indonesia

- **Prita Mulyasari** versus RS. Omni International
- Penyebaran Video Porno **Ariel-Luna-Cut Tari**.
- Mengacaukan proses tabulasi suara di **KPU**
- Steven Haryanto pembuat situs aspal **BCA**. klikbca.com (situs asli Internet banking BCA), menjadi klik-bca.com, kilkbca.com, clikbca.com, klickca.com. dan klikbac.com
- **Carding** oleh mahasiswa Bandung terhadap pihak merchant Jerman
- Deface website2 Malaysia pada kasus **Ambalat, Tarian Tor-tor.**
- Deface website **Presiden SBY (presidensby.info)**

2. TEKNIK HACKER

Kegiatan Hacker

- Pengintaian *(Reconnaissance)*
- Mencari Celah *(Scanning)*
- Ambil Alih Akses *(Gainning Access)*
- Mempertahankan sistem *(Maintaining Access)*
- Menghapus jejak *(Covering Tracks)*

Alasan melakukan Hacking

- **Kepuasan diri** : berhasil melawan sistem yang lebih besar
- **Kejahatan ekonomi** : perampokan bank, penipuan transaksi, pencucian uang, pencurian surat berharga dll)
- **Kejahatan sosial** : pencemaran nama baik, merusak citra, pembunuhan karakter, kebohongan publik dll)
- **Terorisme** : menyerang objek – objek vital negara seperti perusahaan listrik, instalasi militer, kepolisian, pusat transportasi publik, jaringan keuangan perbankan dll.
- **Intelejen** :untuk pertahanan dan keamanan negara

Tipe Hacker

- **Black Hats**. Kumpulan individu dengan keahlian tinggi komputer untuk melakukan tindakan destruktif terhadap sistem demi mendapat imbalan. Disebut juga *crackers.*
- **White Hats**. Kumpulan profesional dengan keahlian tinggi komputer untuk menjaga sistem komputer dari tindakan penyerang. Disebut juga *security analyst.*
- **Gray Hats**. Kumpulan individu yang kadang defensive dan offensive terkait dengan keamanan jaringan.

- **Suicide Hackers**. Kumpulan individu dengan misi utama menyerang objek vital kenegaraan. Mereka tidak khawatir terhadap ancaman perdata dan pidana.

Kerawanan sistem yang sering dimanfaatkan Hacker

- **Sistem Operasi**: seperti : Windows, Mac, Linux, Unix, Android dll
- **Aplikasi :** software dengan extensi *.exe dan patch
- **Modul Program :** *.dll, scripts, drivers.
- **Configurasi :** *.ini, *.cfg, *.reg

Model Serangan di dunia Maya

1. **Malware (Malicious Software) :** program untuk menyusup ke dalam sistem, dengan tujuan merugikan pemilik sistem. Dampaknya: komputer lambat, sistem error, data hilang atau rusak.
- **Virus** - Triggered by User: Overwriting virus, Prepending Virus, Appending Virus, File Infector Virus, Boot Sector Virus, Multipartitive Virus, Macro Virus.
- **Worm:** Virus + Automatic Trigger yang mampu mereplikasi diri sendiri untuk merusak sistem dan jaringan.
- **Trojan Horse:** berupa file – file yang tidak berbahaya seperti *.mp3 ,*.jpg, upgrade software tetapi sebenarnya di dalamnya terdapat virus. Akibatnya: Remote Access Trojan, Password Sending Trojan, FTP port 21 trojan, Proxy Anonymous Trojan.

2. **Web Deface** : Merubah tampilan atau Data
3. **SQL Injection** : exploitasi celah keamanan pada level database
4. **CSS** (Cross Site Scripting): mengacaukan website dinanis melalui kode javascript atau form yang tersedia
5. **Denial of Service (DoS)** : meniadakan layanan / services sistem sehingga pengguna tidak dapat menggunakan layanan tersebut. Misal: disconnect, spam, memory full.
6. **Botnet (Robot Network)**: Program atau script kecil yang menyusupkan bersama virus. Pada waktu tertentu setelah menyebar script akan bekerja sesuai perintah sang *master of puppets.*
7. **Phishing** : proses *pre-attack* dengan cara menyamar sbg pihak yang dipercaya. Dikategorikan sebagai usaha *social engineering* yang memanfaatkan kelemahan pada sifat manusia. Penipu bisa berkedok sebagai *user* penting, *user* sah /legal, mitra vendor, konsultan audit, penegak hukum. Teknik Phishing lain melalui SMS dan pop-up windows

Memanfaatkan Pendekatan Manusiawi (Social Engineering)

- **Rasa Takut** : terhadap pimpinan, penegak hukum dll.
- **Rasa Percaya**: terhadap teman baik, sejawat, saudara, sekretaris dll.
- **Rasa ingin menolong** : terhadap orang yang tertimpa musibah, kesedihan, bencana dll.
- **Rasa Senang dipuji**
- **Rasa Senang Gratis**

Teknik Hacking Pendekatan Manusiawi (Social Engineering)

- Skimming & Camera Pengintai di ATM
- Cari info di tong sampah perusahaan
- Menyamar menjadi Office Boy
- Masuk ke dalam ruangan dengan mengintip pemilik akses legal
- Pura-pura lupa bawa ID-Card ke satpam
- Membantu bawa dokumen, tas & laptop pimpinan
- Add Friend & Chatting

Target Hacker Social Engineering

- Receptionist/ Help Desk/ Front Office
- Admin Komputer
- Mitra kerja/Partner/vendor
- Karyawan Baru

3. ANTISIPASI HACKER

Selain mengantisipasi kemungkinan Hacking melalui lingkungan fisik dan Social engineering berikut ini hal yang perlu dilakukan secara teknologi Informasi (IT):

Pengamanan Data / Informasi

A. Password
B. Encrypted file system / data
C. Anti Virus Software
D. Firewalls & Intrusion Detection System (IDS)
E. Patches & Update
F. Tutup Port yang tidak digunakan
G. Backup Data secara Rutin

A. Password

Password Yang Baik

- Mudah diingat tetapi sulit ditebak orang lain
- 8-15 Character
- Campuran huruf besar, kecil, angka & symbol
- Tidak ada di kamus bahasa
- Beda sistem beda password
- Bahasa alay: 5ul4w351, d3516n, 54yh3ll0
- Singkatan kalimat / lirik lagu favorit

Password Yang Buruk

- Nama plus tahun lahir: Bambang1945
- Kata yang diulang: galau galau
- Membalik nama / kata: darmaji menjadi ijamrad
- Menghilangkan huruf vokal dari nama: bambang sukoco menjadi bbgskc
- Karakter berurut di Keyboard : qwerty, asdfgh, 123456.

Menjaga password

- Jangan simpan di mobile gadget (kecuali di encrypt)
- Hindari save password di mobile gadget
- Jangan beritahu password ke siapapun termasuk admin system
- Pastikan tidak ada CCTV di belakang anda
- Logout jika meninggalkan komputer
- Gunakan Protected Password Screen Saver
- Bersihkan meja dari catatan kecil
- Ganti Password secara periodik

B. Encryted File / Kriptografi

Adalah merubah data menjadi kode / sandi yang tidak bisa dibaca, kecuali dengan menggunakan algoritma / rumus tertentu.

C. Anti Virus

Menggunakan anti virus Lokal & Luar Negeri

D. Firewalls & IDS

Menggunakan firewall di sistem operasi untuk mencegah data – data yang tidak dikenal keluar masuk

E. Patches & Update

H. Tutup Port yang tidak digunakan

Perangkat yang terpasang di komputer menggunakan port tertentu termasuk modem dan LAN.

G. Backup Data secara Rutin

Hal-hal penyebab kebocoran data

- Perilaku masyarakat yang senang berbagi data tentang teman / kerabatnya. Misal: Facebook, twitter, blog, youtube dll
- Ceroboh, tidak tahu mengelola data rahasia. Misal: Data kartu kredit, pinjam ATM
- Teknik Social Engineering untuk menipu. Misal: Hadiah via SMS.
- Jasa Service handphone / gadget & install hardware & software
- Manajer / Admin komputer Pindah Kerja
- Rekaman Rapat
- Digitalisasi data anggota: Reuni, alumni, komunitas
- Internal lebih dominan dari External
- Search Engine yang meluas dan cerdas

Kesimpulan

- “There’s no patch for human stupidity”. Lubang kerawanan software dapat ditutup dengan Patch. Tapi lubang kerawanan pada manusia harus ditutup dengan **Edukasi** IT**.**
- Perlu adanya **Cyberlaw**

4. TEKNIK FORENSIK

Adalah teknik untuk mengumpulkan bahan bukti dari media penyimpanan digital, yang kemudian dapat digunakan secara sah sebagai alat bukti di pengadilan.

Tantangan / Hambatan

- Ilmu masih baru dan masih ‘Learning by doing’. Sehingga lebih banyak ‘Art’ daripada ‘Science’
- Sedikit pelatihan, sertifikasi dan SDM
- Perkembangan media, software & hardware yang begitu pesat
- Alat yang mahal

5. REKAYASA VISUAL

Untuk mengetahui bagaimana memeriksa keaslian suatu data diperlukan pengetahuan juga bagaimana merekayasa dengan software yang biasa dipakai. Agar hoax lebih meyakinkan perlu didukung data-data multimedia seperti Still image, video, audio dan teks. Para Desainer Grafis berpotensi untuk membuat suatu berita bohong/ tersebut. Beberapa teknik yang bisa dipakai antara lain: compositing Image, effects, cloning, video tracking, dubbing dll.

6. UPAYA PEMERINTAH

Untuk menangani Cyber Crime, lembaga pemerintah yang ada yaitu **Cyber Crime Unit** di Mabel Polri dan Indonesia Security Incident Response Team on Inter Security **(ID-SIRTII)** yang berada di bawah Departemen Komunikasi & Informasi (Depkominfo).
Di bawah ID-SIRTII terdiri dari banyak kelompok kecil (bisa pemerintah atau swasta) yaitu Computer Emergency Response Team **(CERT)**.

******** *Semoga Bermanfaat* ******
Salam**: Hendi Hendratman ST**
www.hendihen.com