"Aku lebih menghargai
orang yang **BERADAB**
daripada **BERILMU**.
Kalau hanya berlimu
IBLIS pun lebih tinggi
ilmunya daripada
~~MALAIKAT~~ **MANUSIA**."

Syekh Abdul Qadir Al-Jailani

Cyber Crime

Latar Belakang

- ICT memberikan kemudahakan, efisiensi dan efektivitas pada proses bisnis maupun dalam kehidupan manusia sehari-hari
- Bahkan ICT membuka horison/wawasan baru dalam hal:
  - E-Lifestyle
  - E-Business
  - E-Government
  - E-Entertainment
- Sebaliknya:
  - Proses bisnis semakin bergantung kepada ICT
  - Digital-divide semakin besar (bukan hanya yang melek internet tapi juga yang tahu tapi tidak mengerti benar)
  - Menarik bibit-bibit kejahatan untuk beroperasi
- Karena:
  - knowledge/experience-gap
  - Business mengharuskan tugas-tugas tertentu
  - Terlalu cepat mengaplikasikan teknologi tanpa memikirkan implikasinya terhadap sosial-psikologi

Pengertian Dasar

- Istilah Dasar
  - Cyber: Prefix untuk hal-hal yang berhubungan dengan internet
  - Threat: ancaman
  - Crime: kejahatan
- Hasil Akhir
  - Kerugian oleh pihak lain dan sekaligus keuntungan bagi pihak yang melakukannya
  - Pelanggaran etika (ruang dan waktu)
- Accidents/Kecelakaan
  - Tidak sengaja
  - Random
  - Kerugian (sorted): jiwa, materi, trauma, reputasi, waktu

Pengertian Dasar

- Incidents / kejadian-kejadian:
  - Disengaja (Intentional)
  - Persistence (terus menerus)
  - Kerugian (sorted): materi, waktu, reputasi
- Attact: penyerangan dan perlakuan ke arah terjadinya insiden
- Ancaman: hal-hal yang membawa ke arah terjadinya insiden

Sejarah

- 3500 SM – Komputer sudah dikenal (China, India : Simpoa)
- Charles Babbage's difference engine
- 1820 : Cyber-crime pertama
  - Joseph-Marie Jacquard
    (Mesin tekstil untuk efisiensi kerja, kemudian menemukan compiler digital yang digunakan oleh IBM untukpengembangan komputer modern
  - Pegawai membuat sabotase
- PD-II, jika invasi Jerman dianggap kejahatan, maka penggunaan ENIGMA masuk cyber-crime (ilmu hitam)
- 1972 : Born of internet (ARPA-Net)
- 1978 : First SPAM : Gary Thuerk, Digital Equipment Corp. Marketing executive
- 1980 : RootKit : memperoleh root (admin) di Unix atau Linux
- 1982 : Elk Cloner Virus (FloppyDisk)

Sejarah

- 1983 : Group Milwaukee hackers (the 414's) masuk dalam sistem komputer Los Alamos Laboratories dan Manhattan's Memorial Sloan-Kettering Cancer Center. Penangkapan oleh FBI
- 1988, Robert T. Morris, Jr.,
  - Master – Cornell University, anak dari ilmuwan NSA (National Security Agency) – sekarang Prof. Di MIT
  - Membuat virus di ARPANET yang dapat mereplikasi diri
  - Kerugian : 10-100 juta dollar
  - 1989, Joseph Papp, membuat Trojan dalam database AIDS
- 1996, Phising diperkenalkan alt.2600.hacker newsgroup
- 1998, NSA mengidentifikasi Man-in-the-middle Attack
- 1999, Penyerangan besar-besaran Judi-Online, Bank, dll
- 2000, Denial of Service (DoS) Attack – MafiaBoy (CA)
- 2003, SoBig Worm memanfaatkan BotNet untuk DdoS

Sejarah

- 2006/7, Hackers masuk ke dalam sistem broker besar US
- 15 Desember 2006, saham Apparel Manufacturing Associates dijual hanya 6 cent - kekacauan di stock market
- 2008 – ???

Cyber – 6 Menurut Prof Richardus Eko Indrajit

- Cyber Space
- Cyber Threat
- Cyber Attack
- Cyber Security
- Cyber Crime
- Cyber Law

Cyber Crime

Cyber Crime : Sebuah Evolusi Kejahatan Jenis kejahatan "konvensional":

- Kejahatan kerah biru (blue collar crime)
  Pencurian, penipuan, pembunuhan
- Kejahatan kerah putih (white collar crime)
  Kejahatan korporasi, kejahatan birokrat, malpraktek dll

Karakteristik Unik dari Cybercrime

- Ruang lingkup kejahatan
- Sifat kejahatan
- Pelaku kejahatan
- Modus kejahatan
- Jenis kerugian yang ditimbulkan

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Unauthorized Access
  Terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
  Probing dan Port Scanning merupakan contoh dari kejahatan ini.
  Aktivitas "Port scanning" atau "probing" dilakukan untuk melihat servis-servis apa saja yang tersedia di server target.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Illegal Contents
  - Merupakan 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.
  - Salah satu contoh kasus illegal content yang sering ditemui adalah dalam bidang pornografi (cyberporn). Cyberporn itu sendiri merupakan kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul dan mengekspos hal-hal yang tidak pantas.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Penyebaran Virus Secara Sengaja
  Penyebaran virus umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Contoh kasus : Virus Mellisa, I Love You, dan Sircam.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Data Forgery Kejahatan jenis ini bertujuan untuk memalsukan data pada dokumen-dokumen penting yang ada di Internet.
- Cyber Espionage, Sabotage and Extortion Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki system jaringan komputer pihak sasaran. Selanjutnya, 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.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Cyberstalking
  Dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail, facebook, twitter dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai terror yang ditujukan kepada seseorang dengan memanfaatkan media internet.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Carding
  Merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.
- Hacking dan Cracking
  Istilah hacker biasanya mengacu pada seseorang yang mempunyai minat besar untuk mempelajari system computer secara detail dan bagaimana meningkatkan kapabilitasnya. Besarnya minat yang dimiliki seorang hacker dapat mendorongnya untuk memiliki kemampuan penguasaan system di atas rata-rata pengguna. Jadi, hacker memiliki konotasi yang netral. Aktivitas cracking di internet memiliki lingkungan yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran.

Jenis Cyber Crime

Berdasarkan Jenis Aktivitasnya

- Cybersquatting dan 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.
  Typosquatting adalah kejahatan dengan membuat domain yang mirip dengan nama domain orang lain.
- Hijacking
  Merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak)
- Cyber Terorism
  Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

Jenis Cyber Crime

Berdasarkan Motif Kejahatannya

- Sebagai tindakan murni kriminal
  Kejahatan yang murni merupakan tindak criminal yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding.
- Cybercrime sebagai kejahatan "abu-abu"
  Pada jenis kejahatan di internet yang masuk dalam "wilayah abu-abu" cukup sulit menentukan apakah itu merupakan tindakan criminal atau bukan, mengingat motif kegiatannya terkadang bukan untuk berbuat kejahatan. Contohnya adalah probing atau portscanning.

Jenis Cyber Crime

Berdasarkan Sasaran Kejahatannya

- Menyerang Individu (Against Person)
  Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau criteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain : Pornografi, Cyberstalking, Cyber Tresspass
- Menyerang Hak Milik (Against Property)
  Cybercrime yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Contoh: carding, cybersquatting, typosquatting, hijacking, data forgery
- Menyerang Pemerintah (Against Government)
  Cybercrime Against Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah

Faktor-Faktor Yang Mempengaruhi Terjadinya Cyber Crime

- Faktor Politik
- Faktor Ekonomi
- Faktor Sosial Budaya
  - Kemajuan Teknologi Informasi
  - Sumber Daya Manusia
  - Komunitas Baru

Dampak Cybercrime Terhadap Keamanan Negara

- Kurangnya kepercayaan dunia terhadap Indonesia
- Berpotensi menghancurkan negara

Macam-macam Cyber Crime

- Financial-Fraud
  - Cheating, credit card frauds, money laundering
- Cyber-Pornography
  - Human-trafficking, paedophiles, dll
- Penjualan barang-barang ilegal
  - Lelang cocaine, senjata, bomb, dll
- Online-Gambling
  - Haram pada daerah tertentu, money-laundering
- Intellectual property crime
  - Pembajakan software
  - Pelanggaran trademark
  - Pencurian source code program
- Email Spoofing
  - Potensi konflik
  - Penyerangan terhadap reputasi

Macam-macam Cyber Crime

- Forgery (Pemalsuan)
  - Uang, perangko, materai, stempel
  - Tanda-tangan (termasuk spoofing)
- Cyber-Defamatory (Pemfitnahan)
  - Penyebaran fakta palsu melalui email
  - Analisis yang memutarbalikkan fakta di Blog
- Cyber-Stalking
  - Meneror seseorang dengan email, chat, forum

Teknik Cyber Crime

- Attact/Penyerangan:
  - Syntatic: penyerangan dengan memanfaatkan teknologi
  - Semantic: penyerangan dengan memanfaatkan manusia
- Unauthorized Access:
  - Pencurian Username/Password
  - Masuk dalam sistem (cracking) dengan memanfaatkan vulnerabilities (kelemahan sistem)
  - Contoh:
    - Penggunaan Rootkit (local exploit)
    - Buffer-Overflow (remote / local exploit)
    - SQL – Injection (remote exploit)
- Pencurian data:
  - Fisik: pencurian HD, Flasdisk, USBStick
  - Non-Fisik: unauthorized access

Teknik Cyber Crime

- Denial of Service (DoS)
  - Mengirimkan permintaan pelayanan dalam jumlah besar dan dalam waktu singkat (dan mungkin dari berbagai macam sumber)
  - Contoh: Email Bombing, Multiple http request, Distributed DoS (DdoS), BotNET
- Virus / Worm:
  - Hanya ada di Windows
  - Contoh: Macro, LoveLetter, Melissa & Logic Bombs
- Trojan Attack
  - Semacam virus yang baru berjalan setelah user secara tidak sengaja menjalankannya
  - Ada di Linux (tapi sangat jarang)
- Pemanfaatan kelemahan TCP/IP (authentication)
  - Identify Theft
  - Email spoofing
  - Domain Hijacking

Apa yang harus saya lakukan?

- Peningkatan kesadaran akan adanya cybercrime
- Usaha semua pihak:
  - Pemerintah:
    - UU tentang cybercrime, telematika, hak-cipta, perlindungan privasi
    - Law enforcement knowledge & awareness
  - Pengguna
    - Peningkatan kesadaran (awareness)
    - Up-to-date dengan perkembangan teknologi
  - Ilmuwan/akademisi:
    - Pemikiran-pemikiran baru tentang cybercrime
    - Prediksi tentang implikasi perkembangan teknologi ke masyarakat
    - Interdicipline method: ilmu baru tentang cybercrime, forensic, psikologi, sosiologi
  - Bisnis:
    - Pikirkan juga dampak teknologi tersebut ke masyarakat dan customer jangan hanya memikirkan keuntungan financial saja.

RootKit

- Rootkit adalah program komputer rahasia yang dirancang untuk menyediakan akses istimewa yang berkesinambungan ke komputer sambil secara aktif menyembunyikan kehadirannya. Istilah Rootkit adalah koneksi dari dua kata "root" dan "kit." Awalnya, rootkit adalah kumpulan alat yang memungkinkan akses tingkat administrator ke komputer atau jaringan. Root mengacu pada akun Admin pada sistem Unix dan Linux, dan kit mengacu pada komponen perangkat lunak yang mengimplementasikan alat tersebut. Rootkit Hari ini umumnya terkait dengan malware - seperti Trojans, worm, virus - yang menyembunyikan keberadaan dan tindakan mereka dari pengguna dan proses sistem lainnya.

RootKit

- Rootkit memungkinkan seseorang untuk mempertahankan perintah dan kontrol atas komputer tanpa pengguna / pemilik komputer mengetahuinya. Setelah rootkit diinstal, pengontrol dari rootkit memiliki kemampuan untuk mengeksekusi file dari jarak jauh dan mengubah konfigurasi sistem pada mesin host. Rootkit di komputer yang terinfeksi juga dapat mengakses file log dan memata-matai penggunaan pemilik komputer yang sah

Phishing

- Phishing adalah kejahatan dunia maya di mana target dihubungi melalui email, telepon, atau pesan teks oleh seseorang yang menyamar sebagai lembaga yang sah untuk memikat individu agar memberikan data sensitif seperti informasi identitas pribadi, perincian perbankan dan kartu kredit, dan kata sandi.
- Informasi tersebut kemudian digunakan untuk mengakses akun-akun penting dan dapat mengakibatkan pencurian identitas dan kerugian finansial.

Phishing

- Gugatan phishing pertama diajukan pada tahun 2004 terhadap seorang remaja California yang menciptakan tiruan dari situs web "America Online". Dengan situs web palsu ini, ia dapat memperoleh informasi sensitif dari pengguna dan mengakses detail kartu kredit untuk menarik uang dari akun mereka. Selain phishing melalui email dan situs web, ada juga 'vishing' (phishing suara), 'smishing' (Phishing SMS), dan beberapa teknik phishing lainnya yang terus menerus dilakukan oleh penjahat cyber.

Spoofing

- Serangan spoofing adalah ketika pihak yang jahat meniru perangkat atau pengguna lain di jaringan untuk meluncurkan serangan terhadap host jaringan, mencuri data, menyebarkan malware, atau memotong kontrol akses. Ada beberapa jenis serangan spoofing yang dapat digunakan oleh pihak jahat untuk mencapai hal ini. Beberapa metode yang paling umum termasuk serangan spoofing alamat IP, serangan spoofing ARP dan serangan spoofing server DNS.

Spoofing

- IP address spoofing adalah salah satu metode serangan spoofing yang paling sering digunakan. Dalam serangan IP address spoofing, penyerang mengirim paket IP dari alamat sumber palsu (atau "palsu") untuk menyamarkan dirinya sendiri. Serangan Denial-of-service sering menggunakan spoofing IP untuk membebani jaringan dan perangkat dengan paket yang tampaknya berasal dari alamat IP sumber yang sah.

Makanan yang sedap ada diruang tamu
Orang yang beradap sudah pasti berilmu