Cyber-Threat / Crime

Mata Kuliah
Etika & Profesionalisme TSI
Dosen: Avinanta Tarigan

Latar Belakang

- ICT memberikan kemudahan, efisiensi, & efektivitas pada proses bisnis maupun dalam kehidupan manusia sehari2
- Bahkan ICT membuka horison baru:
  - E-Lifestyle
  - E-Business
  - E-Government
  - E-Entertainment
- Tetapi :
  - 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-too-demanding task force
  - „kesusu“ ... terlalu cepat mengaplikasikan teknologi tanpa memikirkan implikasinya thd sosial - psikologi

Pengertian Dasar

- Istilah Dasar
  - Cyber- ... prefix u/ hal2 yg berhubungan dg 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 disengaja
  - Random
  - Kerugian(sorted): jiwa, materi, trauma, reputasi, waktu
- Incidents:
  - Disengaja (Intentional)
  - Persistence
  - Kerugian(sorted): materi, waktu, reputasi, trauma, jiwa
- Attack: penyerangan & perlakuan ke arah terjadinya insiden
- Ancaman: hal2 yang membawa ke arah terjadinya insiden

Sejarah

- 3500 SM – Komputer sdh dikenal (China, India: Simpoa)
- Charles Babbage's difference engine
- 1820 : Cyber-crime pertama
  - Joseph-Marie Jacquard
  - mesin tekstil untuk efisiensi pekerjaan.
  - pegawai membuat sabotase
- PD-II, jika invasi Jerman dianggap kejahatan, maka penggunaan ENIGMA masuk cybercrime (ilmu hitam)

- 1972: Born of Internet (ARPA-Net)
- 1978: First SPAM: Gary Thuerk, Digital Equipment Corp. marketing executive
- 1980: RootKit: gaining root (admin) in Unix
- 1982: Elk Cloner Virus (FloppyDisk)
- 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

Sejarah

- 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 dolar
- 1989, Joseph Papp. Membuat Trojan dalam database AIDS
- 1996, Phising diperkenalkan alt.2600.hacker newsgroup
- 1998, NSA identifies 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
- 2006/7, Hackers masuk ke dalam sistem broker besar US
  - 15 Des 06, saham Apparel Manufacturing Associates dijual hanya 6 cent - kekacauan di stock market
- 2008 ???? buuuuanyak lagi

Macam-macam Cybercrime

- 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 Crima
  - Pembajakan software
  - Pelanggaran trademark
  - Pencurian source code program
- Email Spoofing
  - Potensi konflik
  - Penyerangan thd reputasi

Macam-macam Cybercrime

- 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 dg email, chat, forum

Teknik Cybercrime

- Attack / Penyerangan:
  - Syntatic: penyerangan dg memanfaatkan teknologi
  - Semantic: penyerangan dg 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, FlashDisk, USBStick
  - Non-Fisik: unauthorized access

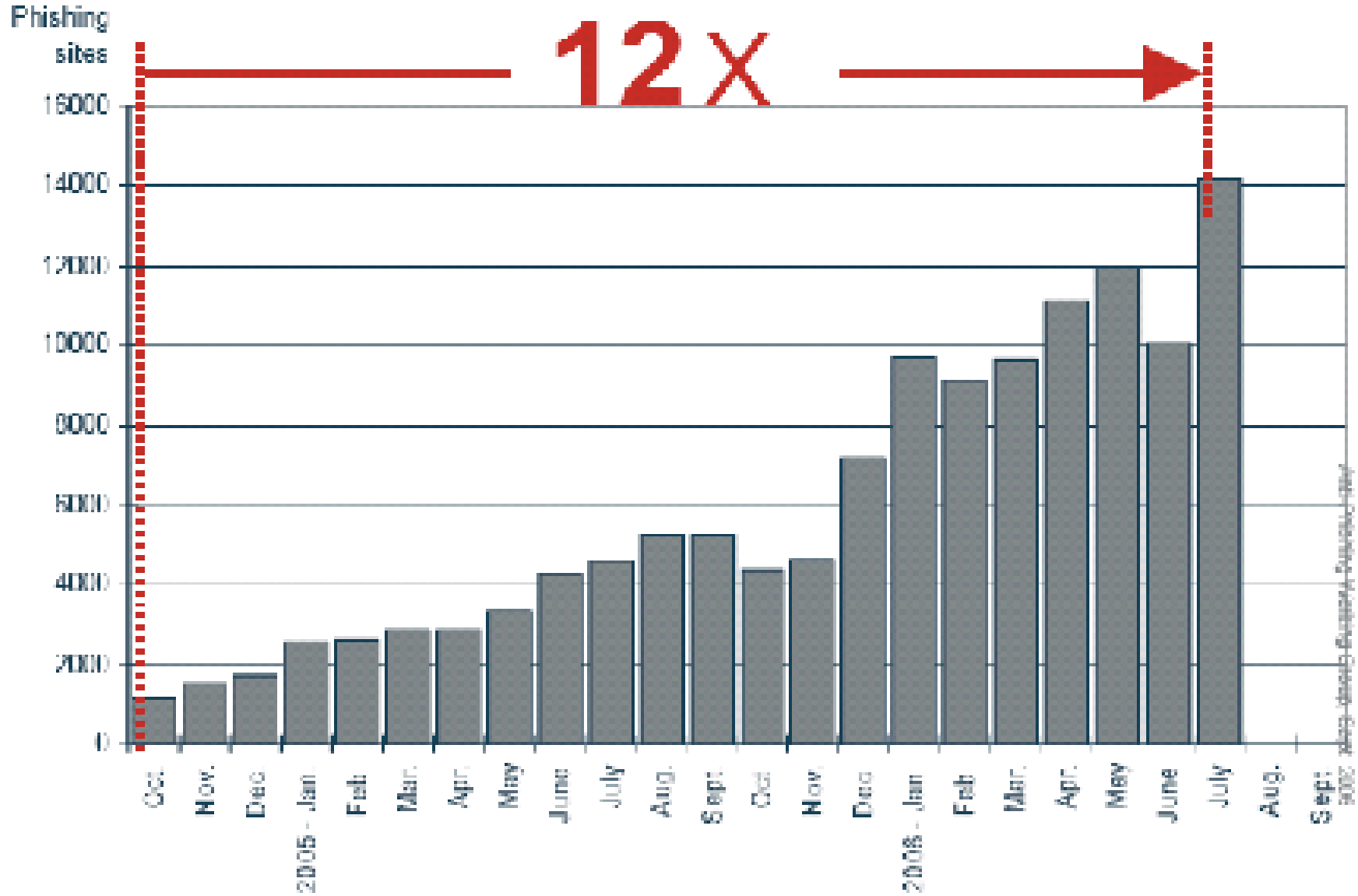
Teknik Cybercrime

- 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)

Teknik Cybercrime

- Pemanfaatan kelemahan TCP/IP (authentication):
  - Identity Theft
  - Email spoofing
  - Domain Hijacking
  - Site-phising
- Pemanfaatan kelemahan protocol / program:
  - Session Hijackers (man-in-the-middle attack)
  - KeyLoggers
- Social Engineering:
  - Memanfaatkan ketidaktahuan user
  - Vishing: penjahat menelepon untuk mendapatkan data
  - Spear-Phising: penjahat masuk dalam social networking site (e.g. Friendster) untuk mendapatkan data
  - Pura-pura menjadi kawan kencan untuk mendapatkan data (sumber: film-film science fiction)

Peningkatan Cybercrime



http://www.pwgsc.gc.ca/recgen/colloquium2007/

Trus ... bagaimana dong ?

- Peningkatan kesadaran ttg adanya cybercrime dan
- 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:
    - *Pemikiran2 baru ttg cybercrime*
    - *Prediksi ttg implikasi perkembangan teknologi ke masyarakat*
    - *Interdicipline method: Ilmu baru ttg cybercrime, forensic, psikologi, sosiologi*
  - Bisnis:
    - *please dong ... jangan duit mulu ... pikirkan juga impact teknologi tsb ke masyarakat dan customer*