Modul 8

Computer Ethics & Computer Crime

whanz@ukdw.ac.id

Ethical Behaviors?

- That sure is a great music where did you get it?
  - Downloading of music from the web
- Have you given a friend a copy of your Microsoft Project software?
  - Software Piracy
- Did you read the confidential company file that was accidentally attached to your email?
  - Computer abuse
- Did you gain access to the network and invade other workers emails and files?
  - Computer abuse
- You formatted your hard drive prior to leaving your company because you were angry about leaving.
  - Destruction of property

Ethics/Etika

- **Etika** berasal dari bahasa Yunani Kuno: "*ethikos*", yang berarti "timbul dari kebiasaan“
- **Etika** adalah cabang utama filsafat yang mempelajari nilai atau kualitas yang menjadi standar dari penilaian moral.
- **Etika** mencakup analisis dan penerapan konsep seperti benar, salah, baik, buruk, dan tanggung jawab.
- **Etika dan TI?**
  - Adakah yang perlu bertanggung jawab?
  - Adakah yang akan terkena dampaknya?

Computer Ethics

- **Computer Ethics**

  Adalah analisis moral tentang baik-buruk, benar-salah dari tindakan manusia dalam memanfaatkan pengetahuan komputernya mencakup perbuatan terhadap dirinya sendiri, pihak lain dan lingkungannya secara langsung maupun tidak.

- **Pertimbangan Etis**
  - Apakah etis jika kita menggunakan komputer untuk memanipulasi foto dengan cara mempertukarkan foto orang lain
  - Apakah etis jika seorang progammer meletakkan *time bomb* pada programnya supaya pada waktunya kelak program menjadi rusak dan klien selalu bergantung pada programmer
  - Apakah cukup etis menghapus data orang lain dalam komputer bersama tanpa memberi tahu si empunya data
  - Apakah etis seorang staf EDP memberitahu informasi perusahaan yang dia ketahui kepada orang lain yang tidak berhak
  - Apakah etis menginformasi data seseorang (mis: selebritis) untuk tujuan yang bersifat komersial maupun tidak

Computer Ethics - 2

- Isyu Pokok Dalam Computer Ethics yang menimbulkan dilema
  - **Prinsip dasar**

    Untuk memecahkan masalah yang dihadapi klien, maka sebagai seorang profesional perlu memberikan alternatif pemecahan masalah. Dalam beberapa kasus pemecahan masalah ini berakibat pembeberan semua kebenaran termasuk didalamnya kelemahan sistem yang ada hal ini terkadang merugikan klien. Bagaimanakah etika berperanan disini?
  - **Egoisme**

    Dalam hubungan antara klien dan profesional, adakah profesional memandang bahwa klien adalah orang yang tidak-tahu apa-2 dibidang komputer sehingga harus mengikuti apa yang diinginkan oleh profesional. Dengan kata lain profesional mengambil keputusan sepihak tanpa melibatkan si klien

Computer Ethics - 3

- Isyu Pokok ……
  - **Kerahasiaan**
    - Sejauh mana klien dapat menaruh kepercayaan kepada profesional untuk membeberkan semua rahasia perusahaan
    - Sejauh mana profesional dapat dipercaya menjaga kerahasiaan informasi yang diperoleh dari si klien
  - **Hak otonomi klien**
    - Hak dari klien untuk mendapatkan semua informasi yang perlu diketahui dan *source code* dari program yang telah dibuat tanpa ada batasan-2 tertentu
    - Hak dari klien untuk melakukan klaim bila terjadi disfungsi dari program yang dibuat sesuai dengan kesepakatan
    - Hak dari klien untuk bebas dari unsur-2 sabotase terhadap program yang telah dibuat

The Hacker Ethics

- Access to computers and anything which might teach you something about the way the world works should be unlimited and total.
- All information should be free.
- Mistrust authority promote decentralization.
- Hackers should be judged by their hacking, not on the criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

The Ten Commandments

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not use or copy software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you write.
10. Thou shalt use a computer in ways that show consideration and respect.

SIFAT ANCAMAN TERHADAP SISTEM INFORMASI

1. Ancaman Pasif

a. Bencana alam & politik
   - contoh : gempa bumi, banjir, perang, kebakaran

b. Kesalahan Manusia
   - contoh : kesalahan memasukkan & penghapusan data

c. Kegagalan sistem
   - contoh : gangguan listrik, kegagalan peralatan & fungsi software

SIFAT ANCAMAN TERHADAP SISTEM INFORMASI

2. Ancaman Aktif

a. Kecurangan & kejahatan komputer
   - penyelewengan aktivitas
   - penyalahgunaan kartu kredit
   - sabotase
   - pengaksesan oleh orang yang tidak berhak

b. Program yang jahat / usil
   - contoh : virus, cacing, trojan, bom waktu dll

AKAR KEJAHATAN KOMPUTER

- Informasi = Uang?
  - Informasi memiliki nilai (value) yang dapat dijual belikan
    - Data-data nasabah, mahasiswa
    - Informasi mengenai perbankan, nilai tukar, saham
    - Soal ujian
    - Password, PIN
  - Nilai dari informasi dapat berubah dengan waktu
    - Soal ujian yang sudah diujikan menjadi turun nilainya

Kriteria Sebuah Kejahatan

Ada 3 buah skenario:

1. Mr X mencuri printer dari sebuah lab komputer
2. Mr X masuk ke lab komputer (tanpa izin) dan kemudian mengintai
3. Mr X masuk ke lab komputer dimana dia punya izin untuk masuk, dan kemudian menaruh bom untuk mematikan sistem komputer di lab

Apakah Kriteria Kejahatan diatas:?

- Kejahatan di atas tidak akan dapat terjadi apabila teknologi komputer tidak ada
- Apakah ketiga kejahatan di atas bisa dituntut sebagai kejahatan biasa?
- Apakah ketiga kejahatan di atas bisa disebut kejahatan komputer?
- Ketiga kejahatan di atas adalah kejahatan yang biasa terjadi dan bukan kejahatan komputer

Definisi Kejahatan Komputer

- Kapan sebuah tindakan kriminal dianggap sebagai kejahatan komputer?
- Apakah semua kejahatan yang menggunakan komputer bisa dianggap sebagai kejahatan komputer ?
- Apakah orang yang mencuri televisi bisa dianggap sebagai kejahatan televisi ?
- Apakah orang yang mencuri handphone bisa dianggap sebagai kejahatan handphone ?
- Apa beda antara Computercrime dan Cybercrime?

Definisi Kejahatan Komputer (2)

Skenario lainnya:

1. Mr X marah dan melempar laptopnya ke temannya sehingga sehingga berakibat ybs harus di rawat di rumah sakit
2. Mr X menggunakan komputer untuk menggelapkan pajak penghasilan
3. Mr X menggunakan komputer yang bukan haknya untuk melakukan pengubahan file komputer rekannya

Definisi Kejahatan Komputer:

- Komputer adalah komponen utama yang digunakan Mr X untuk melakukan kejahatannya ?
- Apakah Mr X telah melakukan kejahatan komputer ?
- Girasa (2002) mendefinisikan Kejahatan Komputer sebagai: ***aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama***
- Apakah yang dimaksud dengan komponen utama?
- Tavani (2000) mendefinisikan cybercrime sebagai ***kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber***

Computer Crime Category

- **Credit Card Fraud**
  - Pemanfaatan secara tidak sah kartu kredit orang lain
  - Masyarakat perlu mendapat perlindungan hukum dan teknologi
- **Computer and Data Communication Fraud**
  - Meliputi spektrum kejahatan yang sangat luas mulai dari kegiatan memasuki jaringan komputer orang lain sampai dengan mengambil data yang ada di jaringan
  - Pemanfaatan jaringan kantor untuk kepentingan pribadi
  - Pemanfaatan komputer untuk memindahkan dana secara ilegal.
- **Unauthorized access to computer files (*Cybertrespass)***
  - Penggunaan komputer orang lain secara tidak sah
  - Mengakses record data yang bersifat confidential dengan tujuan mencuri
  - Memindahkan dan mengganti data untuk keuntungan pribad

Computer Crime Category - 2

- **Unlawful copying of copyrighted Software (*Cyberpiracy*)**
  - Men-*sharing*-kan software yang memiliki copyright
  - Mengcopy software yang memiliki copyright tanpa seiijin produsen yang sah
  - Meniru dan menggunakan hasil karya orang lain yang bercopyright untuk kepentingan pribadi/komersial
- **Sexual harrasment and abusement**
  - Memanipulasi gambar orang lain untuk tujuan pelecehan sexual dan pornografi
  - Menggunakan anak-2 dibawah umur untuk tujuan komersial pornography
  - Tidak menyediakan filter untuk mencegah anak usia dibawah umur mengunjungi situs-situs porno
- **Transmitting Computer virus to destroy data (*Cybervandalism)***
  - Menggunakan virus komputer utk mencuri data orang lain
  - Menggunakan virus komputer sebagai *time bomb*
  - Menggunakan virus komputer utk merusak data

Penyidikan dan Tuntutan Hukum

- Tuntutan hukum bagi kejahatan komputer relatif sulit karena:
  - Belum adanya perangkat hukum dan undang-2 kejahatan komputer khususnya di negara berkembang.
  - Indonesia baru saja memiliki UUITE, tetapi belum dapat di implementasikan karena belum ada PPnya
  - Hampir sebagian besar kejahatan komputer tidak terdeteksi dan jika diketahui bukan karena penyilidikan melainkan secara kebetulan
  - Penegakan hukum lemah karena aparat penegak hukum: polisi, hakim dan jaksa tidak menguasai kompleksitas kejahatan komputer (white collar crime) karena merupakan kejahatan dengan memanfaatkan teknologi tinggi, sementara banyak aparat penegak hukum yang *computer illiterate*

Cybercrime vs Cyber-Related Crime

- Banyak kejahatan yang menggunakan teknologi komputer tidak bisa disebut *cybercrime*
- Pedophilia dan pornografi bisa disebarkan dengan atau tanpa menggunakan *cybertechnology* sehingga hal-hal di atas tidak bisa disebut *cybercrime*
- Kejahatan yang dapat dilakukan dengan atau tanpa bantuan *cybertechnology* disebut *cyber-related crime*

Phising

From: <USbank-Notification-Urgecq@UsBank.com>
To: …
Subject: USBank.com Account Update URGEgb
Date: Thu, 13 May 2004 17:56:45 -0500

USBank.com

Dear US Bank Customer,
During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
http://www.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage

Note: Requests for information will be initiated by US Bank Business Development; this process cannot be externally requested through Customer Support.

SECURITY BREACH ACCIDENT (1)

1996	*U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di system komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan
1996	*FBI National Computer Crimes Squa*d, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan
1997	Penelitian *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Inggris, *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US $30.000 / insiden.
1998	FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti *(convicte*d) di pengadilan naik 88% dari 16 ke 30 kasus.
	Dan lain-lain. Dapat dilihat di www.cert.org

SECURITY BREACH ACCIDENT (2)

1988	Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai *"denial of service attack"*. Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.
10 Maret 1997	Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts. http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv
1990	Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.
2000	Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <http://www.2600.com>
2000	Wenas, membuat server sebuah ISP di singapura down

Kesadaran Keamanan

- Mengapa Keamanan Komputer dibutuhkan?
  - *"information-based society*", menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,
  - Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hol*e)

Kesadaran Keamanan (2)

- Kejahatan Komputer semakin meningkat karena:
  - Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
  - Desentralisasi server.
  - Transisi dari single vendor ke multi vendor.
  - Meningkatnya kemampuan pemakai (user).
  - Kesulitan penegak hukum dan belum adanya perundang-undangan..
  - Sistem terhubungan dengan jaringan Internet.

SECURITY ATTACK MODELS

- ***Interruption***
  Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem. Contoh serangan adalah “denial of service attack”.
- ***Interception***
  Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretappin*g).
- ***Modification***
  Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- ***Fabrication***
  Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Pelaku Kejahatan Komputer

- Information bandit
  - Sekarang masih dipotretkan sebagai jagoan
  - Akan tetapi akan berkurang
  - *the disappearance act of information bandits*
- Information security professionals
  - Masih kurang
  - Lebih menyenangkan
- Keduanya menggunakan tools yang sama
- Perbedaannya sangat tipis: itikad & pandangan
- **Jangan bercita-cita menjadi bandit!**

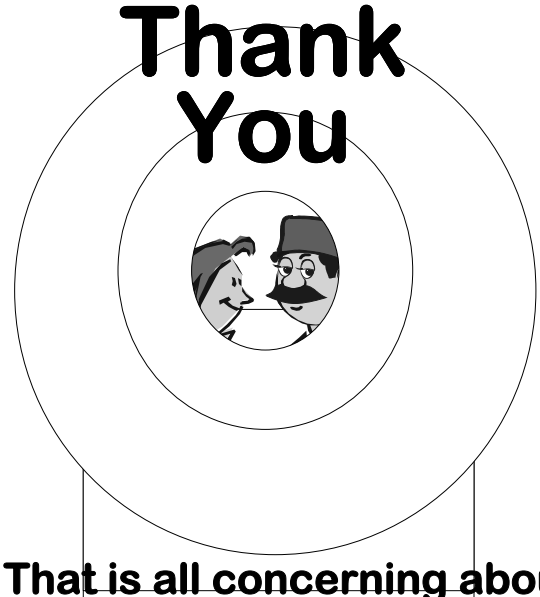
Karakteristik Penyusup

- **The Curious (Si Ingin Tahu)**
  Tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
- **The Malicious (Si Perusak)**
  Tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
- **The High-Profile Intruder (Si Profil Tinggi)**
  Tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
- **The Competition (Si Pesaing)**
  Tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup

- **Mundane:** tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- **Lamer (script kiddies):** mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- **Wannabe:** paham sedikit metode hacking, dan sudah mulaiberhasil menerobos sehingga berfalsafah; HACK IS MY RELIGION.
- **Larva (newbie):** hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
- **Hacker:** aktivitas hacking sebagai profesi.
- **Wizard:** hacker yang membuat komunitas pembelajaran di antara mereka.
- **Guru:** master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

Thank You



That is all concerning about Computer Crime