Security in Electronic Communication

Ancaman pada Sistem Komputer dan Komunikasi

- Survei yang telah dilakukan bahwa pengguna internet tidak memiliki "pengetahuan" tentang keamanan online sehingga mereka rentan menjadi korban kejahatan onlineHasil survei Microsoft 83% responden di Indonesia menghadapi berbagai resiko online.
- Hanya 3% yang menyatakan secara proaktif melindungi diri dari resiko tersebut (Chandrataruna, 2013).
- Hanya 28% responden pengguna desktop, dan
- 32% pengguna perangkat mobile (Yusuf, 2013)

Kategori dan Jenis Ancaman Pada Sistem Komputer dan Komunikasi

Kategori Ancaman	Jenis Ancaman
Kesalahan dan Kecelakaan	Kesalahan manusiaKesalahan prosedurKesalahan perangkat lunakMasalah elektromekanisMasalah "data kotor"
Bencana Alam	Kebakaran, banjir, gempa bumi, tornado, badai, dsb
Kejahatan Komputer	Pencurian perangkat keras, Pencurian perangkat lunak, Pencurian musik dan film online, Pencurian waktu dan layanan, Pencurian informasi, Penyalahgunaan yang berhubungan dengan internet, Pengambilalihan PC: zombie, botnet, dan blackmail, Kejahatan yang dapat merusak keseluruhan sistem
Pelaku Kejahatan Komputer	Individu atau kelompok kecilPegawaiRekan bisnis dan pemasok dari luarMata-mata perusahaanLayanan intelijen asingKejahatan terorganisasiTeroris

Kesalahan dan kecelakaan

- **Kesalahan manusia** → Manusia kerap tidak mampu menilai kebutuhan informasi mereka sendiri Emosi manusia mempengaruhi performa Manusia bertindak berdasarkan persepsi mereka yang acap kali tidak mampu mengimbangi laju informasi.
- **Kesalahan Prosedural** → Kesalahan Perangkat Lunak Berkaitan dengan istilah "bug", artinya suatu kesalahan pada program yang menyebabkan program tersebut tidak bekerja dengan baik

Kesalahan dan Kecelakaan

- Masalah "Data Kotor"

  Data kotor adalah data yang tidak lengkap, kadaluarsa atau tidak akurat

- Masalah Elektromekanik

  Sistem mekanik, misalnya printer dan sistem elektronik tidak selalu dapat bekerjaAda kalanya perangkat-perangkat tersebut mengalami kesalahan konstruksi, terkena kotoran, atau terlalu panas, usang, atau rusak karena sebab yang lain

Bencana Alam

- Bencana alam merupakan jenis kerusakan yang dapat menghancurkan keseluruhan sistem.
- Apapun yang berbahaya bagi properti (dan manusia) juga berbahaya bagi sistem komputer dan komunikasi
- Contoh: kebakaran, banjir, gempa bumi, tornado, badai, badai salju, dan sebagainya

Kejahatan Komputer

- Pencurian perangkat keras
- Pencurian perangkat Lunak
  - Misalnya pembajakan software
  - Di Indonesia, rasio pembajakan software (piranti lunak) mencapai sekitar 86% pada tahun 2011
- Pencurian Musik dan Film Online
- Pencurian Waktu dan Layanan

  Misal orang menggunakan waktu komputer perusahaan untuk bermain game, melakukan belanja online, atau menelusuri web pornografi.

Kejahatan Komputer

- Pencurian Informasi

  Misalnya mencuri rekaman pribadi yang penting, dan menjual informasi tersbut

- Penipuan di Internet

  penipuan saat pelelanganpembayaran yang tidak dikirimpenipuan kartu kredit atau kartu debitpenipuan cekpenipuan investasipenipuan kepercayaanpenipuan identitas

Kejahatan Komputer

- **Pengambilalihan PC**
  Penyerang pengambilalih komputer tapi ijin user asli
- **Kejahatan Motif Pribadi**
  Didasari kepuasan batin dan motif balas dendam

Pelaku Kejahatan Komputer

Individu atau kelompok kecil	• Misalnya phiser, pharmer, kreator spyware dan virus, craker dan hacker
Pegawai	• Hasil survei ancaman pada infrastrkutur teknologi karena serangan dunia maya adalah pegawai yang masih aktif (53%), mantan pegawai (10%), dan nonpegawai (28%) (CSO Magazine survey, 2002)Pegawai bisa menggunakan teknologi informasi untuk keuntungan pribadi atau mencuri perangkat keras atau informasi untuk dijual

Pelaku Kejahatan Komputer

- Mitra dan Pemasok dari luar
- Mata-mata perusahaan misalnya untuk mendapatkan rahasia dagang yang bisa mereka gunakan untuk keunggulan bersaing
- Layanan Inteligent Asing
- Kejahatan Terorganisasi
- Teroris

Pengamanan Komputer dan Komunikasi

Keamanan

Sistem penjagaan keamanan untuk melindungi teknologi informasi dari kerusakan, kegagalan sistem, dan akses yang tidak berwenang yang bisa mengakibatkan kehancuran dan kerugian

Lima komponen keamanan

- Mencegah kejahatan komputer
- Identifikasi dan akses
- Enkripsi
- Melindungi perangkat lunak dan data
- Rencana pemulihan dari bencana

Mencegah Kejahatan Komputer

Memperkuat Hukum	• UU mengenai TI
CERT	• Computer Emergency Response Team • CERT menyediakan informasi internasional dan layanan dukungan seputar keamanan bagi para pengguna internet
ID-SIRTI	• Indonesia Security Incident Response Team on Intenet and Infrastrukture/Coordination Center • Bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet

Klasifikasi Kejahatan Komputer

David Icove

- Keamanan yang bersifat fisik (physical security)
- Keamanan yang berhubungan dengan orang (personel):
- Keamanan dari data dan media serta teknik komunikasi (communications)
- Keamanan dalam operasi

Aspek / servis dari security

Privacy
Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses

Integrity
Menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi

Authenttication
Berhubungan dengan metode untuk menyatakan bahwa informasi betul2 asli

Availability
Berhubungan dengan ketersediaan informasi ketika dibutuhkan

Identifikasi dan Akses

- Sistem Komputer ingin mengetahui apakah betul Kita orang yang mempunyai akses sah
- Sistem mencoba mengotentikasi identitas Kita dengan menentukan
  - Apa yang Kita Miliki: Kartu, Kunci, Tanda tangan, dan Kartu Identitas
  - Apa yang Kita Ketahui: Pin dan Password
  - Siapa Kita: Ciri-ciri Fisik

Enkripsi

- Enkripsi adalah proses mengubah data yang bisa dibaca ke dalam bentuk yang tidak bisa dibaca untuk mencegah akses dari orang yang tidak berhak
- Kebanyakan komputer pribadi telah menggunakan bentuk enkripsi yang sangat canggih

Melindungi Perangkat Lunak dan Data

Kontrol Akses
- Akses ke file online dibatasi hanya bagi mereka yang memiliki hak akses yang sah

Kontrol Audit
- Jaringan memiliki kontrol audit untuk melacak program atau server mana yang digunakan, file mana yang dibuka, dan seterusnya

Kontrol Orang
- Mengingat orang merupakan ancaman terbesar pada sistem komputer, maka usaha pencegahan dimulai dengan menyaring pelamar kerja

Perencanaan Pemulihan dari Bencana

- Rencana pemulihan dari bencana tersebut meliputi daftar semua fungsi bisnis, perangkat keras, perangkat lunak, data, dan orang-orang yang mendukung fungsi tersebut serta pengaturan untuk lokasi-lokasi alternatif.

- Rencana itu juga menyertakan cara mem-backup data dan menyimpan program dan data di lokasi lain, serta cara menyiapkan sekaligus melatih personel yang diperlukan.


Thank you
THE END OF PRESENTATION