PENGANTAR
Keamanan Sistem Informasi

Pendahuluan

- Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*".
- Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi).
- Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi.

Data Internet (Tahun 2010)

EMAIL

- * 107 trilyun - Jumlah emails yang dikirim melalui inernet dalam 2010.
- * 294 milyar- Rata -rata pesan email setiap harinya.
- * 1.88 milyar - Jumlah pengguna Email diseluruh dunia.
- * 480 juta - Pengguna Email baru di Tahun 2010.
- * 89, 1 % - Jumlah spam emails per hari.
- * 2.9 milyar - Jumlah akun email diseluruh dunia.

PENGGUNA INTERNET

- * 14% - peningkatan pengguna inet semenjak tahun 2009 diseluruh dunia.
- * 825.1 juta - pengguna inet di Asia
- * 475.1 juta - pengguna inet di Eropa
- * 266.2 juta - pengguna inet di Amerika Utara
- * 204.7 juta - pengguna inet di Amerika Latin
- * 110.9 juta - pengguna inet di Africa
- * 63.2 juta - pengguna inet di Asia Tengah
- * 21.3 juta - pengguna inet di Australia (oceania)

SOCIAL MEDIA

- * 152 juta - Jumlah bLOG di Internet (berdasrkan tracking BLOGPULSE)
- * 25 milyar - jumlah twitters pada tahun 2010
- * 100 juta - Jumlah akun baru di tahun 2010
- * 175 juta - jumlah orang yang ada di twitter (sampai September 2010)
- * 7.7 juta - jumlah orang yang mem follow LADY GAGA
- * 600 juta - jumlah akun di facebook sampai tahun 2010
- * 250 juta - jumlah orang baru di facebook tahun 2010
- * 30 milyar - jumlah konten yang dibagikan di FACEBOOK setiap bulannya
- * 70 % - pembagian facebook user berdasarkan lokasi diluar Amerika
- * 20 juta - jumlah applikasi facebook yang diinstal setiap harinya

PICTURES

- * 5 milyar - jumlah poto di Flickr (sampai september 2010)
- * lebih dari 3000 - jumlah poto yang diplod di flick setiap menitnya
- * 130 juta - Jumlah rata-rata photo yang di uplod di flickr tiap bulannya.
- * lebih dari 3 milyar - Jumlah foto yang di uplod di FACEBOOK setiap bulannya
- * 36 milyar - jumlah foto yang diuplod di facebook setiap tahunnya.

WEBSITES

- * 255 juta - Jumlah websites sampai dengan Desember 2010
- * 21.4 juta - penambahan webstites dalam 2010

Data Internet (Tahun 2010)

Keamanan dan Managemen Perusahaan

- Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating) atau, paling tidak, mendeteksi adanya* penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.
- Survey Information Week (USA), 1271 system or network manager, hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting.
- Meskipun sering terlihat sebagai besaran yang tidak dapat langsung diukurdengan uang (*intangible), keamanan sebuah sistem informasi sebetulnya* dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible).*

Keamanan dan Managemen Perusahaan

TABLE 1. Kontribusi terhadap Risk

Nama komponen	Contoh dan keterangan lebih lanjut
Assets (aset)	• hardware • software • dokumentasi • data • komunikasi • linkungan • manusia
Threats (ancaman)	• pemakai (*users*) • teroris • kecelakaan (*accidents*) • crackers • penjahat kriminal • nasib (*acts of God*) • intel luar negeri (*foreign intelligence*)
Vulnerabilities (kelemahan)	• software bugs • hardware bugs • radiasi (dari layar, transmisi) • tapping, crosstalk • *unauthorized users* • cetakan, *hardcopy* atau print out • keteledoran (*oversight*) • cracker via telepon • storage media

Untuk menanggulangi resiko (*Risk)* *tersebut dilakukan apa yang disebut "countermeasures" yang dapat berupa:*

- **usaha untuk mengurangi *Threat***
- **usaha untuk mengurangi *Vulnerability***
- **usaha untuk mengurangi impak (*impact)***
- **mendeteksi kejadian yang tidak bersahabat (*hostile event)***
- **kembali (*recover) dari kejadian***

Statistik Sistem keamanan

- Di Inggris, 1996 *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Survey ini juga menunjukkan bahwa kerugian yang diderita rata-rata US $30.000 untuk setiap insiden. Ditunjukkan juga beberapa organisasi yang mengalami kerugian sampai US $1.5 juta.
- 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 (*convicted*) di pengadilan

- 7 Februari 2000 (Senin) sampai dengan Rabu pagi, 9 Februari 2000. Beberapa web terkemuka di dunia diserang oleh "*distributed denial of service attack*" (DDoS attack) sehingga tidak dapat memberikan layanan (down) selama beberapa jam. Tempat yang diserang antara lain: Yahoo!, Buy.com, eBay, CNN, Amazon.com, ZDNet, E-Trade. FBI mengeluarkan tools untuk mencari program TRINOO atau Tribal Flood Net (TFN) yang diduga digunakan untuk melakukan serangan dari berbagai penjuru dunia.

Statistik Sistem keamanan di Indonesia

- Januari 2000. Beberapa situs web Indonesia diacak-acak oleh cracker yang menamakan dirinya "fabianclone" dan "naisenodni" (indonesian dibalik). Situs yang diserang termasuk Bursa Efek Jakarta, BCA, Indosatnet. Selain situs yang besar tersebut masih banyak situs lainnya yang tidak dilaporkan.
- Seorang cracker Indonesia (yang dikenal dengan nama hc) tertangkap di Singapura ketika mencoba menjebol sebuah perusahaan di Singapura.
- September dan Oktol
  kembali Fabian Clon
  Perlu diketahui bahv
  banking.
- **Juni 2001.** Seorang pengguna Internet Indonesia membuat beberapa situs yang mirip (persis sama) dengan situs klikbca.com, yang digunakan oleh BCA untuk memberikan layanan Internet banking. Situs yang dia buat menggunakan nama domain yang mirip dengan klikbca.com, yaitu kilkbca.com (perhatikan tulisan "kilk" yang sengaja salah ketik), wwwklikbca.com (tanpa titik antara kata "www" dan "klik"), clikbca.com, dan klickbca.com. Sang user mengaku bahwa dia medapat memperoleh PIN dari beberapa nasabah BCA yang salah mengetikkan nama situs layanan Internet banking tersebut.
- **16 Oktober 2001.** Sistem BCA yang menggunakan VSAT terganggu selama beberapa jam. Akibatnya transaksi yang menggunakan fasilitas VSAT, seperti ATM, tidak dapat dilaksanakan. Tidak diketahui (tidak diberitakan) apa penyebabnya. Jumlah kerugian tidak diketahui.

Meningkatnya Kejahatan Komputer

- Jumlah kejahatan komputer (*computer crime), terutama yang berhubungan* dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain:
  - Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat.
  - Desentralisasi (dan *distributed) server menyebabkan lebih banyak* sistem yang harus ditangani.
  - Transisi dari *single vendor ke multi-vendor sehingga lebih banyak* sistem atau perangkat yang harus dimengerti dan masalah *interoperability antar vendor yang lebih sulit ditangani.*
  - Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya (atau sistem milik orang lain).
  - Mudahnya diperoleh software untuk menyerang komputer dan jaringan komputer.
  - Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.
  - Semakin kompleksnya sistem yang digunakan seperti semakin besarnya program (*source code) yang digunakan sehingga semakin* besar probabilitas terjadinya lubang keamanan (yang disebabkan kesalahan pemrograman, bugs).
  - Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti Internet. Hal ini membuka akses dari seluruh dunia.

Klasifikasi Kejahatan Komputer

- Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying). Menurut David Icove [18]* berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:
  - Keamanan yang bersifat fisik (*physical security)*
  - Keamanan yang berhubungan dengan orang (personel)
  - Keamanan dari data dan media serta teknik komunikasi
  - Keamanan dalam operasi

Aspek / servis dari security

A computer is secure if you can depend on it and its software to behave as you expect. (Garfinkel and Spafford)

- Garfinkel [15] mengemukakan bahwa keamanan komputer *(computer security) melingkupi empat aspek, yaitu privacy, integrity, authentication,* dan availability. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce, yaitu* access control dan non-repudiation.
  - **Privacy / Confidentiality :** Inti utama aspek *privacy atau confidentiality adalah usaha untuk menjaga* informasi dari orang yang tidak berhak mengakses.
  - **Integrity** Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
  - **Authentication** Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.
  - **Availability** Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
  - **Access Control** Aspek ini berhubungan dengan cara pengaturan akses kepada informasi.
  - **Non-repudiation** Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Serangan Terhadap Keamanan Sistem Informasi

- Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings [40] ada beberapa kemungkinan serangan (*attack):*

  - *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah "denial of service attack".
  - *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
  - *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.

Electronic commerce: mengapa sistem informasi berbasis Internet

- Sistem informasi saat ini banyak yang mulai menggunakan basis Internet. Ini disebabkan Internet merupakan sebuah platform yang terbuka (*open platform) sehingga menghilangkan ketergantungan perusahaan pada sebuah* vendor tertentu seperti jika menggunakan sistem yang tertutup (*proprietary systems). Open platform juga mempermudah interoperability antar vendor.*
- Selain alasan di atas, saat ini Internet merupakan media yang paling ekonomis untuk digunakan sebagai basis sistem informasi. Hubungan antar komputer di Internet dilakukan dengan menghubungkan diri ke link terdekat, sehingga hubungan fisik biasanya bersifat lokal. Perangkat lunak (*tools) untuk menyediakan sistem informasi berbasis Internet (dalam bentuk* server web, ftp, gopher), membuat informasi (HTML editor), dan untuk mengakses informasi (web browser) banyak tersedia. Perangkat lunak ini banyak yang tersedia secara murah dan bahkan gratis.
- Alasan-alasan tersebut di atas menyebabkan Internet menjadi media elektronik yang paling populer untuk menjalankan bisnis, yang kemudian dikenal dengan istilah electronic commerce (e-commerce). Dengan diperbolehkannya bisnis menggunakan Internet, maka penggunaan Internet menjadi meledak. Statistik yang berhubungan dengan kemajuan Internet dan e-commerce sangat menakjubkan.

Electronic commerce: mengapa sistem informasi berbasis Internet

Statistik Internet

Jumlah komputer, server, atau lebih sering disebut *host* yang terdapat di Internet menaik dengan angka yang fantastis. Sejak tahun 1985 sampai dengan tahun 1997 tingkat perkembangannya (*growth rate*) jumlah host setiap tahunnya adalah 2,176. Jadi setiap tahun jumlah host meningkat lebih dari dua kali. Pada saat naskah ini ditulis (akhir tahun 1999), growth rate sudah turun menjadi 1,5.

Data-data statistik tentang pertumbuhan jumlah host di Internet dapat diperoleh di "Matrix Maps Quarterly" yang diterbitkan oleh MIDS[1]. Beberapa fakta menarik tentang Internet:

- Jumlah host di Internet Desember 1969: 4
- Jumlah host di Internet Agustus 1981: 213
- Jumlah host di Internet Oktober 1989: 159.000
- Jumlah host di Internet Januari 1992: 727.000

Electronic commerce: mengapa sistem informasi berbasis Internet

Statistik Electronic Commerce

Hampir mirip dengan statistik jumlah host di Internet, statistik penggunaan Internet untuk keperluan e-commerce juga meningkat dengan nilai yang menakjubkan. Berikut ini adalah beberapa data yang diperoleh dari International Data Corporation (IDC):

- Perkiraan pembelian konsumer melalui Web di tahun 1999: US$ 31 billion (31 milyar dolar Amerika). Diperkirakan pada tahun 2003 angka ini menjadi US$177,7 billion.
- Perkiraan pembelian bisnis melalui web di tahun 1999: US$80,4 billion (80,4 milyar dolar Amerika). Diperkirakan pada tahun 2003 angka ini menjadi US$1.1 trillion.
- Jika diperhatikan angka-angka di atas, maka e-commerce yang sifatnya bisnis (*business to business*) memiliki nilai yang lebih besar dibandingkan yang bersifat *business to consumer*.

Keamanan Sistem Internet

Untuk melihat keamanan sistem Internet perlu diketahui cara kerja sistem Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa sistem (router, gateway, hosts, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan [32]. Kelemahan sebuat sistem terletak kepada komponen yang paling lemah.

Asal usul Internet kurang memperhatikan masalah keamanan. Ini mungkin dikarenakan unsur kental dari perguruan tinggi dan lembaga penelitian yang membangun Internet. Sebagai contoh, IP versi 4 yang digunakan di Internet banyak memiliki kelemahan. Hal ini dicoba diperbaiki dengan IP Secure dan IP versi 6.

Hackers, Crackers, dan Etika

- Untuk mempelajari masalah keamanan, ada baiknya juga mempelajari aspek dari pelaku yang terlibat dalam masalah keamanan ini, yaitu para hackers and crackers
- Istilah hackers sendiri masih belum baku karena bagi sebagian orang hackers mempunyai konotasi positif, sedangkan bagi sebagian lain memiliki konotasi negatif. Bagi kelompok yang pertama (*old school), untuk* pelaku yang jahat biasanya disebut *crackers. Batas antara hacker dan* cracker sangat tipis. Batasan ini ditentukan oleh etika.

- Serangan dari hackers Portugal yang mengubah isi beberapa web site milik pemerintah Indonesia dikarenakan hackers tersebut tidak setuju dengan apa yang dilakukan oleh pemerintah Indonesia di Timor Timur. Selain mengubah isi web site, mereka juga mencoba merusak sistem yang ada dengan menghapus seluruh disk (jika bisa).
- Serangan dari hackers Cina dan Taiwan terhadap beberapa web site Indonesia atas kerusuhan di Jakarta (Mei 1998) yang menyebabkan etnis Cina di Indonesia mendapat perlakukan yang tidak adil. Hackers ini mengubah beberapa web site Indonesia untuk menyatakan ketidak-sukaan mereka atas apa yang telah terjadi.
- Beberapa hackers di Amerika menyatakan akan merusak sistem milik pemerintah Iraq ketika terjeadi ketegangan politik antara Amerika dan Irak.

TUGAS 1 - INDIVIDU

- Buat ESSAI (Tulisan Ilmiah) 3-5 Halaman
- Tema “ Pentingnya Keamanan Data dan Informasi”
- Menyangkut latar belakang, Analisis, teknik, metode keamanan, kasus, hal-hal yang ingin dicapai dan dislesaikan.
- Dikumpulkan Paling Lambat hari Sabtu 28 Maret 2020, melalui KULIAH ONLINE
- Referensi dari jurnal, artikel ilmiah , tulis diakhir essai (10-15 Jurnal nasional / internasional – Penulisan mengikuti standar IEEE)
- Tulis pada cover Tugas Tugas MK Keamanan Sistem Informasi , NIM, NAMA, LOGO UNIKOM, PRODI dan UNIKOM serta Tahun Tugas

Merci bien
ありがとう
Matur Nuwun
Hatur Nuhun
Obrigado
Dank
Thanks
Matur se Kelangkong
Syukron
Kheili Mamnun
ευχαριστιες
Danke
Grazias
谢谢
Terima Kasih


Irawan_afrianto@yahoo.com

Irawan.afrianto

@Irawan_afrianto

+628170223513