Mengamankan Sistem Informasi

Gentisya Tri Mardiani, S.Kom

Cara Pengamanan

- Pemantau integritas sistem
- Audit
- Backup secara rutin
- Penggunaan enkripsi

Pemantau Integritas Sistem

- Pemantau integritas sistem dijalankan secara berkala untuk menguji integratitas sistem.

- Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire.*
- Program paket *Tripwire* dapat digunakan untuk memantau adanya perubahan pada berkas.

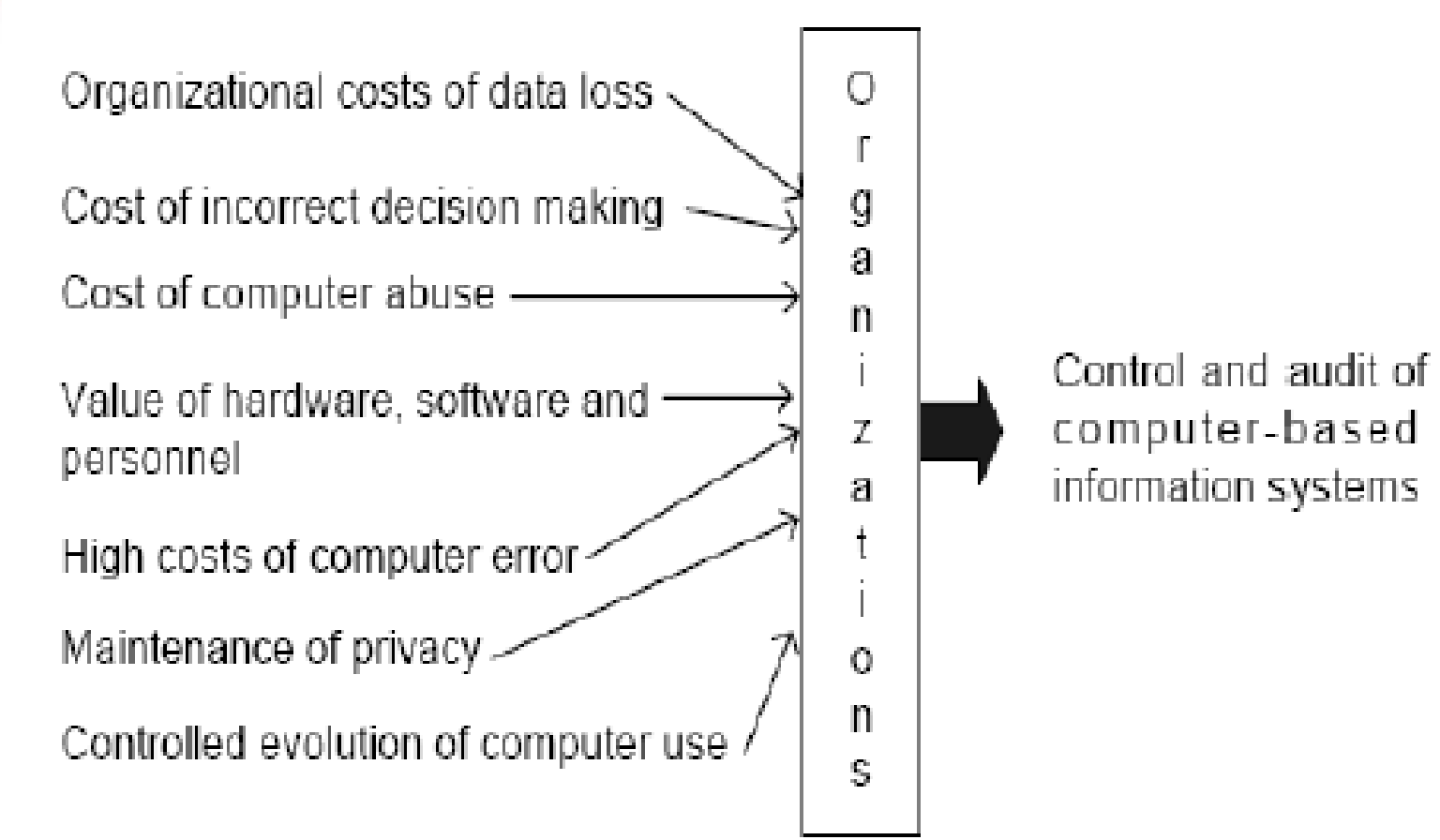
Audit

- Audit adalah proses yang sistematis, independen, dan terdokumentasi untuk mendapatkan bukti, kemudian dilakukan evaluasi untuk menentukan sejauh mana kriteria audit terpenuhi.

Audit Teknologi Informasi

- Secara garis besar, audit TI dilakukan untuk menilai:
  - Apakah sistem informasi terkomputerisasi dapat mendukung pencapaian tujuan organisasi/ perusahaan
  - Apakah sistem informasi suatu organisasi/ perusahaan dapat mendukung pengamanan aset
  - Apakah penggunaan sistem terkomputerisasi pada organisasi/ perusahaan telah dikelola secara efisien

Audit TI


Organizational costs of data loss
Cost of incorrect decision making
Cost of computer abuse
Value of hardware, software and personnel
High costs of computer error
Maintenance of privacy
Controlled evolution of computer use
Organizations
Control and audit of computer-based information systems

Tujuan Audit TI

- Pengamanan Aset
  seluruh aset berupa hardware, software, SDM harus dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset

- Menjaga integritas data

- Efektifitas
  suatu sistem informasi dikatakan efektif jika sistem tersebut telah sesuai dengan kebutuhan user

Tujuan Audit TI

- Efisiensi
  efisiensi dalam desai dan penggunaan sistem informasi, berkaitan dengan efektifitas dan sisi ekonomis penggunaan sumber daya

- Ekonomis
  perhitungan dan pertimbangan *benefit-cost ratio*

Area Audit TI

- **Perencanaan**
  bagaimana rencana harus dikelola sesuai tujuan.
- **Organisasi dan manajemen**
  fungsi manajerial dan pengelolaan institusi yang baik
- **Kebijakan dan prosedur**
  pembentukan kebijakan dan prosedur yang baku
- **Keamanan**
  pengamanan terhadap aset penting perusahaan
- **Regulasi dan standar**
  kesesuaian dan keselarasan regulasi, hukum dan aturan yang mendukung standar berjalannya kinerja perusahaan

Pihak yang diaudit TI

- Manajemen
- Divisi IT (manajer, network, DBA, system analyst, proggrammer, dll)
- User

Pelaku Audit

- Internal Audit
  dilakukan oleh atau atas nama perusahaan sendiri biasanya untuk management review atau tujuan internal perusahaan
- Lembaga independen di luar perusahaan
  - Second party audit
    dilakukan oleh pihak yang memiliki kepentingan terhadap perusahaan
  - Third party audit
    dilakukan oleh pihak independen dari luar perusahaan,misalnya untuk sertifikasi

Electronic Data Processing Audit

- Audit Pengolahan Data Electronik (PDE) merupakan bentuk pengawasan dan pengendalian dari infrastruktur teknologi secara menyeluruh

- Pada awalnya hanya mengacu pada audit pemrosesan data saja, kemudian meluas ke seluruh SI

- Dipakai untuk menentukan apakah aset sistem informasi perusahaan telah digunakan secara efektif dan integratif dalam mencapai tujuan organisasi

Jenis Audit PDE

- **Application System**
  verivikasi untuk memastikan kebenaran, kehandalan, kecepatan, maupun keamanan data pada saat pengiriman, pemrosesan serta pengeluaran informasi

- **Information Processing Facilities**
  terkait dengan fasilitas yang digunakan untuk mengolah informasi

- **System development**
  kontrol pengembangan sistem dalam suatu organisasi

Jenis Audit PDE

- **IT Management**
  audit yang dilaksanakan untuk memastikan apakah lingkungan/ komponen organisasi dalam pemrosesan informasi dilakukan secara terkendali dan efisien

- **Network**
  memastikan kehandalan jaringan komnikasi yang digunakan sesuai dengan kebutuhan dan proses bisnis yang berjalan.

Audit: mengamati berkas log

- Segala (sebagian besar) kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut "*logfile*" atau *"log"*.

- Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Misalnya kegagalan untuk masuk ke sistem (login), tersimpan di dalam berkas log.

- Para administrator diwajibkan untuk rajin memelihara dan menganalisa berkas log yang dimilikinya.

Audit: mengamati berkas log

- Letak dan isi dari berkas log bergantung kepada operating system yang digunakan. Di sistem berbasis UNIX, biasanya berkas ini berada di direktori **/var/adm atau /var/log**.

- *Registry* dalam Windows NT, Windows 2000, Windows XP dan Windows Server 2003 disimpan di dalam direktori **%systemroot%\system32\config**.

Audit: mengamati berkas log

Berkas-berkas berikut merupakan berkas *registry* untuk sistem operasi Windows NT, Windows 2000, Windows XP dan Windows Server 2003:

- %systemroot%\system32\config\Sam - HKEY_LOCAL_MACHINE\SAM
- %systemroot%\system32\config\Security - HKEY_LOCAL_MACHINE\SECURITY
- %systemroot%\system32\config\Software - HKEY_LOCAL_MACHINE\SOFTWARE
- %systemroot%\system32\config\System - HKEY_LOCAL_MACHINE\SYSTEM
- %systemroot%\system32\config\Default - HKEY_USERS\.DEFAULT
- %systemroot%\system32\config\Userdiff
- %UserProfile%\Ntuser.dat - HKEY_USERS\<SID> (HKEY_CURRENT_USER)
- %UserProfile%\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat - HKEY_USERS\<SID>_Classes (HKEY_CURRENT_USER\Software\Classes)

Audit: mengamati berkas log

- Contoh berkas log pada sistem Linux Debian

Nama Berkas	Keterangan
/var/adm/auth.log	Berisi informasi yang berhubungan dengan authentication. Gagal login, misalnya, dicatat pada berkas ini.
/var/adm/daemon.log	Informasi mengenai program-program daemon seperti BIND, Sendmail, dsb.
/var/adm/mail.log	Berisi informasi tentang e-mail yang dikirimkan dan diterima serta akses ke sistem email melalui POP dan IMAP.
/var/adm/syslog	Berisi pesan yang dihasilkan oleh program syslog. Kegagalan login tercatat di sini.

Audit: mengamati berkas log

- Contoh isi dari berkas var/adm/auth.log:

```
Apr  8 08:47:12 xact passwd[8518]: password for `inet' changed
by root
Apr  8 10:02:14 xact su: (to root) budi on /dev/ttyp3
```

- Contoh isi yang agak mencurigakan:

```
Apr  5 17:20:10 alliance wu-ftpd[12037]: failed login from
ws170.library.msstate.edu [130.18.249.170], m1
Apr  9 18:41:47 alliance login[12861]: invalid password for
`budi' on `ttyp0' from `ppp15.isp.net.id'
```

Backup secara rutin

- Hal ini dilakukan untuk menghindari hilangnya data akibat bencana seperti kebakaran, banjir, dan lain sebagainya.

- Apabila data-data dibackup akan tetapi diletakkan pada lokasi yang sama, kemungkinan data akan hilang jika tempat yang bersangkutan mengalami bencana seperti kebakaran.

Penggunaan enkripsi

- Data-data yang anda kirimkan diubah sedemikian rupa sehingga tidak mudah disadap mudah oleh program penyadap (*sniffer).*

- Banyak servis di Internet yang masih menggunakan "*plain text"* untuk *authentication,* seperti penggunaan pasangan userid dan password.

Penggunaan enkripsi

- Contoh servis yang menggunakan plain text antara lain:
  - akses jarak jauh dengan menggunakan telnet dan rlogin
  - transfer file dengan menggunakan FTP
  - akses email melalui POP3 dan IMAP4
  - pengiriman email melalui SMTP
  - akses web melalui HTTP

TUGAS KELOMPOK

- Buat sistem informasi yang aman:
  - menerapkan prinsip/ aspek keamanan sistem informasi
  - menerapkan cara mengamankan sistem
  - dapat digunakan sesuai kebutuhan sistem informasi
- Menguji keamanan sistem informasi yang dibuat tersebut:
  - Menggunakan program penyerang, program sniffer, atau
  - Membuat program penyerang,
  - Menguji aspek keamanan sistem informasi

Dikumpulkan laporan, program, dan presentasi.
Waktu 2 minggu.

Thank you