Operations Security

Tujuan

- Mempelajari teknik-teknik kontrol pada operasi personalia SI, sistem informasi dan perangkat keras.

Topik

- Segregation of duties, accountability, personnel hiring practices, input & output controls, change management control, attacks, hacking, intrusion, virus

Categories of Control

- Preventative Control-to lower amount and impact of errors. And to prevent unauthorized intruders.
- Detective controls – to detect error once it has occurred.
- Corrective(recovery) controls-help mitigate impact of a loss
- Deterrent-used to encourage compliance with external controls
- Application-used to minimize and detect software's operational irregularities.
- Transaction-used to provide control over various stages of a transaction.

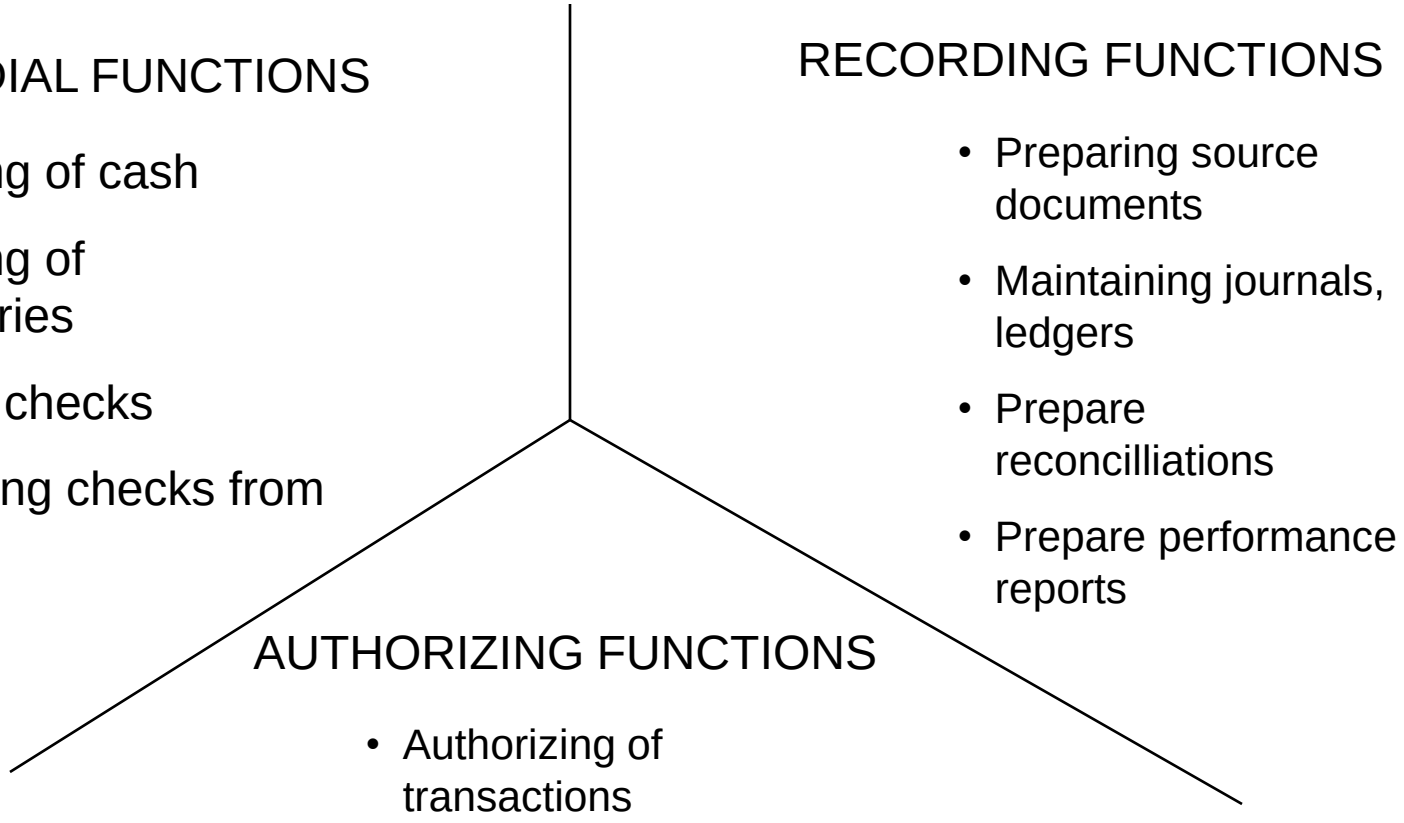
Covert Channel Access

- An info path that is not normally used for communication within a system, therefore it is not protected by the systems normal security mechanisms.
- 2 types:
  - covert storage-convey info by changing a systems stored data
  - covert timing-convey info by altering the performance of or modifying the timing of a system in some measurable way.

Trusted Facility Management

- Defined as the assignment of a specific individual to administer the security related functions of a system.
- Terms that fall under here are
  - least privileged, separation of duties, need to know…

Separation of duties rule (dlm accounting)



Contoh untuk dunia komputer apa kira-kira?

Separation of duties

- Assigns parts of tasks to different personnel → least previlage
- Sebaiknya ada 3 jenis admin:
  - System administrator
  - Security admin
  - Enhanced operator function
- Jika ada yg digabung, harus ada proses audit
- Two-man control: saling mengapprove pekerjaan orang lain
- Dual control: dua orang diperlukan untuk melakukan suatu pekerjaan tertentu
- M-of-N: misalnya untuk root key signing, butuh 5 dari 6 direksi

Segregation of Duties Within the Systems Function

- In a highly integrated system, procedures that used to be performed by separate individuals are combined.
- Any person who has unrestricted access to the computer, its programs, and live data could have the opportunity to both perpetrate and conceal fraud.
- To combat this threat, organizations must implement compensating control procedures.

Segregation of Duties Within the Systems Function

Authority and responsibility must be clearly divided among the following functions:

1. Systems analysis
2. Programming
3. System administrator,
4. Network administrator,
5. Database administrator
6. Users
7. AIS library
8. Data control
9. Security Manager / QA manager
10. System Tester

Segregation of Duties Within the Systems Function

- It is important that different people perform these functions.
- Allowing a person to perform two or more of them exposes the company to the possibility of fraud.

Least Privileged

- Read only-can only read
- Read/Write-cannot change original data
- Access change-can change data in its original location.

Tugas System Administrator

- Install system software
- Booting dan shutdown
- Add/remove user
- Backup & recovery
- Memantau dan mengelola print queue

Sebagian tugas bisa didelegasikan kepada enhanced operator

Tugas Security Admin

- Set user clearence, initial password
- Change security profile
- Change object (file, data, device) security label/level
- Review audit trail data

Rotation of Duties

- Pembatasan periode waktu pekerjaan yang terkait dengan security, untuk dipindahkan ke pekerjaan lain
- Mengurangi kolusi dan penipuan
- Bisa dipaksakan pula konsep *mandatory leave*

Trusted recovery

- Ensures security is not breached when a system crashes.
- Trusted recovery is required only for B3 and A1 level systems.
- Fail secure-system system preservers state in crash
- Terdiri dari 2 tahap:
  - Failure preparation: mirroring, backup, temporary file
  - System recovery
- Beberapa jenis recovery:
  - Manual recovery
  - Automated recovery
  - Automated recovery with undue loss

Configuration / Change Management Control

- The process of tracking and approving changes to a system. Involves identifying, controlling, and auditing all changes made.
- These changes can be hardware, software, or network.
- Configuration/man control can also be used to protect a trusted system while it is being built.
- MAIN GOAL OF CONFIGURATION/CHANGE MAN CONTROL: security not unintentionally diminished!
- Configuration Management **:** Auditing and controlling any changes to the Trusted Computing Base

Administrative Controls

- Controls installed/maintained by admin management to reduce threat or impact of security violation.
- Personnel Security:
  - Employment screening,
  - mandatory vacation time,
  - job warnings.

Record Retention

- Refers to how long transactions and other types of records should be retained. Deals with computer files, directories, and libraries.
- Data remanence-refers to data left on erased media that can be obtained through forensics.

Resource Protection

- Protecting companies resources and assets.
- Some resources that require protection are modem pools, routers, storage media etc..
- Transparency of Controls should be kept in mind when developing security policies.
- Your security should not interfere with users job tasks.
- This also has another reason. The more they directly have to address security issues in their everyday job, the more they learn about the security of the system.

Privileged Entity Controls

- Defined as an extended or special access to computing resources given to operators and sysadmins.
- Many job duties require this.

Media Security Controls

- Logging-logging for accountability
- Access control-to prevent unauthorized personnel
- Proper disposal-destruction of media.

Media Viability Controls

- Marking-proper mark
- Handling-special handling
- Storage-secure, room temp

Monitoring and Auditing

- Problem identification and problem resolution are primary goals of monitoring.
- Monitoring contains the mechanisms, tools, and techniques which permit the identification of security events that could impact the operation of a computer facility.
- These techniques are:
  - Intrusion Detection-used to analyze traffic patters as well as function as IDS
  - Penetration Testing
  - Violation processing using clipping levels-sets a clipping level for normal use

Audit Trails

- Enable the enforcement of individual accountability by creating a reconstruction of events.
- Audit logs should contain: date and time, person, terminal used, and security events.
- In addition, the auditor should also examine the audit logs for the following:
- Re runs, computer operator practices, amendments to production jobs.

Problem management

- To reduce failures to a manageable level
- To prevent occurrence of problem
- To mitigate the negative impact of problems on computing services and resources.

Viruses

Definisi

- "variety of malicious computer programs that send out requests to the operating system, of the host system under attack, to append the virus to other programs."
- In this way, viruses are self-propagating to other programs. They can be relatively benign, such as web application defacement, or malicious, such as deleting files, corrupting programs or causing a denial of service.
- Generally, viruses attack four parts of the computer:
  1. Executable program files
  2. The file-directory system, which tracks the location of all the computer's files
  3. Boot and system areas, which are needed to start the computer
  4. Data files

Kendali Virus

- To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic antivirus program needs to be established.
- There are two major ways to prevent and detect viruses and worms that infect computers and network systems.
  1. by having sound policies and procedures in place, and
  2. by technical means, including antivirus software.
- Neither is effective without the other.

Kendali Prosedural

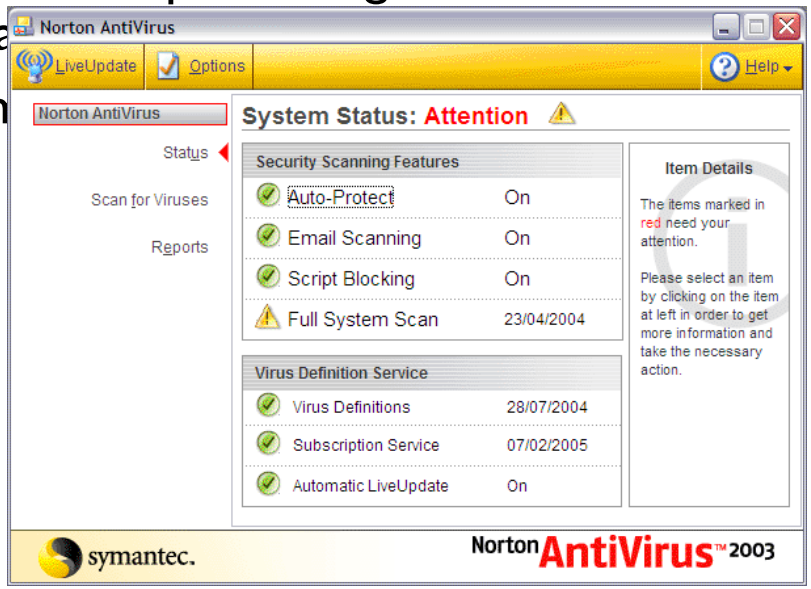
- Instal sistem dari sumber orisinil
- Update virus definitions frequently
- Write protect all media when possible
- Dilarang menjalankan shareware dan freeware kecuali yang sudah diuji
- Penggunaan antivirus pada server-server dan workstation
- Update/patch untuk OS dan peralatan jaringan otentik
- Awareness mengenai virus kepada pengguna, misalnya jangan tergoda dengan email yang "menggoda"
- Ada strategy backup. Juga ada kebijakan untuk menscan backup kalau sistem yang berjalan terkena virus

Kendali Teknis

- Boot virus protection (bisa dari BIOS)
- Remote booting
- Hardware based password
- Penggunaan media yang memiliki proteksi data fisik (misalnya tab pada disket)
- Menutup port-port yang sering diserbu worm dan virus tertentu

Anti Virus

- The most common antivirus tool
- Considered the most effective means of protecting networks and host-based computer systems aga
- Antivirus software should be prin
- Unless updated periodically, antivirus software will not be an effective tool against viruses.
- Antivirus software contains a number of components that address the detection of viruses via scanning technologies from different angles.



Jenis Antivirus

- Scanners, biasanya menggunakan siganture/definitions
- Active Monitors pada level interrupt (terutama dulu di zaman DOS)
- Integrity CRC checkers → ada CRC pada database
- Behavior blockers (mirip seperti active monitors), untuk aktivitas yang tidak biasa seperti format, penulisan pada boot sector, atau mengubah executables
- Immunizers, menambahkan beberapa byte pada executeables.

Spyware

- Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a *spybot* or *tracking software*), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.
- Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.
- However, spyware is often installed without the user's consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window.

- Software designed to serve advertising, known as adware, can usually be thought of as spyware as well because it almost invariably includes components for tracking and reporting user information. However, marketing firms object to having their products called "spyware."
- As a result, McAfee (the Internet security company) and others now refer to such applications as "potentially unwanted programs" (PUP).
- The cookie is a well-known mechanism for storing information about an Internet user on their own computer. If a Web site stores information about you in a cookie that you don't know about, the cookie can be considered a form of spyware. Spyware is part of an overall public concern about privacy on the Internet.
- Many Internet users were introduced to spyware in 1999, when a popular freeware game called "Elf Bowling" came bundled with tracking software.