# Chapter #1

## Ancaman pada Keamanan Informasi

AIK21363 (3 sks)

## Keamanan dan Jaminan Informasi

Information Assurance and Security

Nurdin Bahtiar, M.T

# Materi

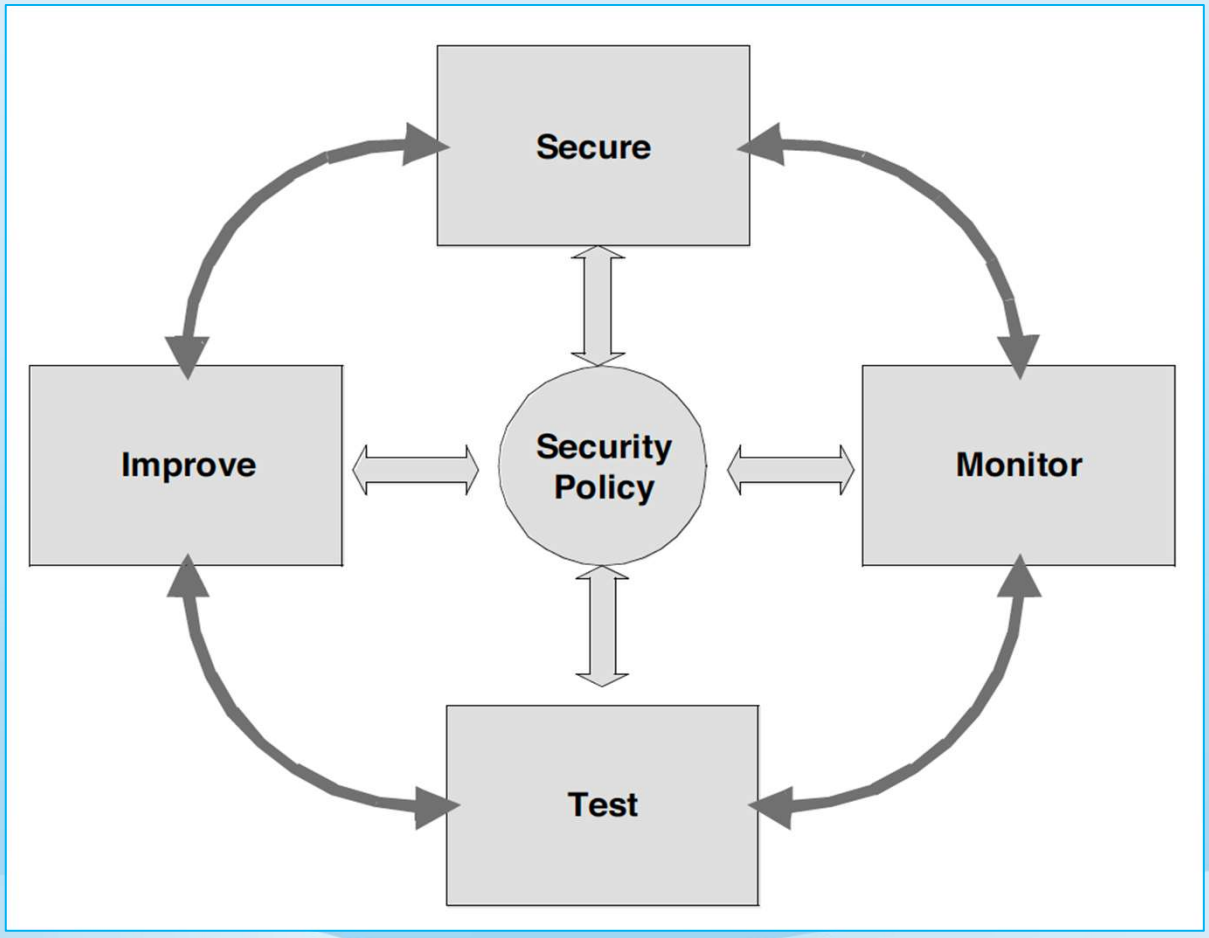
1. What is Information Security?
2. Error and Omissions
3. Fraud and Theft
4. Malicious Hackers
5. Malicious Code
6. Denial-of-Service Attacks
7. Social Engineering

# 1. What is Information Security?

- Hal paling utama dan paling penting terkait keamanan informasi adalah kebijakan keamanan. Andaikan 'keamanan informasi' adalah seorang manusia, maka 'kebijakan keamanan' merupakan sistem saraf pusatnya.
- "*Site Security Handbook*" (RFC 2196) mendefinisikan kebijakan keamanan sebagai "**Pernyataan formal tentang aturan yang harus dipatuhi oleh orang yang diberi akses ke teknologi dan aset informasi organisasi**".
- Aspek lain yang berhubungan dengan keamanan informasi adalah keamanan organisasi, klasifikasi asset, keamanan personal, serta keamanan fisik.*

* Dibahas pada pertemuan-pertemuan selanjutnya.

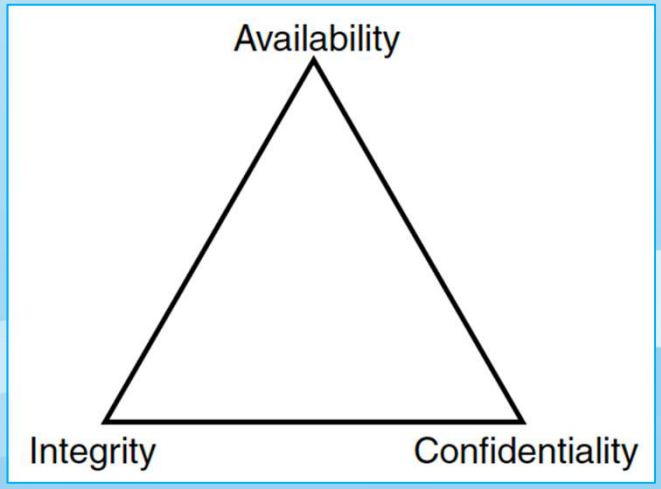
# 1. What is Information Security?




Security Wheel (Peltier, et al)

# 1. What is Information Security?

- Perusahaan memiliki sederetan tujuan dengan diadakannya sistem informasi yang berbasis komputer di dalam perusahaan. Oleh karena itu, perusahaan menuntut agar diciptakan sistem keamanan terhadap hardware maupun softwarenya.
- **Tujuan dari pengamanan** ini adalah untuk meyakinkan integritas, kelanjutan/ketersediaan, dan kerahasiaan dari pengolahan data.
- Reputasi organisasi akan dipandang baik bagi khalayak umum apabila dapat diyakinkan oleh 3 hal:
  1. Integritas informasi
  2. Kerahasiaan informasi
  3. Ketersediaan informasi



CIA triad

# 1. What is Information Security?

ISO-17799 definition:

- ***Confidentiality***: ensuring that information is accessible only to those authorized to have access to it.". This can be one of the most difficult tasks to ever undertake. To attain confidentiality, you have to keep secret information secret.

- ***Integrity***: the action of safeguarding the accuracy and completeness of information and processing methods." This can be interpreted to mean that when a user requests any type of information from the system, the information will be correct.

- ***Availability***: ensuring that authorized users have access to information and associated assets when required. This means that when a user needs a file or system, the file or system is there to be accessed.

# 1. What is Information Security?

- Informasi merupakan aset organisasi yang sangat berharga dan penting seperti halnya asset-asset yang lain seperti mesin, gedung, SDM, dsb.
- Aset-aset yang dapat dimasukkan ke dalam sistem informasi dapat dikategorikan sbb:
  1. Personil
  2. Perangkat keras
  3. Perangkat lunak aplikasi
  4. Perangkat lunak sistem
  5. Data
  6. Fasilitas
  7. Penunjang

# 1. What is Information Security?

- Informasi dapat diklasifikasikan seperti berikut:
  1. ***Top secret***. Bila disebarluaskan akan berdampak sangat parah terhadap keuntungan berkompetisi dan strategi bisnis organisasi.
  2. ***Confidential***. Bila disebarluaskan akan merugikan privasi perorangan, yang berimbas merusak reputasi organisasi.
  3. ***Restricted***. Hanya ditujukan kepada orang-orang tertentu untuk menopang bisnis organisasi.
  4. ***Internal use***. Hanya boleh digunakan oleh pegawai perusahaan untuk melaksanakan tugasnya.
  5. ***Public***. Dapat disebarluaskan kepada umum melalui jalur yang resmi.

# 1. What is Information Security?

- **Ancaman** adalah suatu aksi atau kejadian yang berpotensi dapat merugikan perusahaan / organisasi.
- Kerugian dapat berupa kehilangan uang / biaya, tenaga upaya, peluang bisnis, reputasi, atau bahkan kepailitan.
- Ancaman organisasi dapat disebabkan oleh:
  1. Kegagalan perangkat keras
  2. Kegagalan perangkat lunak
  3. Kegagalan SDM
  4. Alam
  5. Keuangan
  6. Eksternal
  7. Internal

# 2. Error and Omissions (kesalahan dan kelalaian)


- Meskipun kesalahan dan kelalaian manusia bukan merupakan persoalan terkini, tetap saja ia merupakan tantangan utama sistem kita.
- Kita tidak dapat menghalangi komunitas pengguna, sehingga susah untuk kita melindungi sistem dari masuk keluarnya pengguna yang mengaksesnya.
- Kesalahan dan kelalaian tersebut berpotensi menyebabkan hilangnya integritas informasi.

# 2. Error and Omissions


- Untuk mengatasi dampak yang ditimbulkan dari adanya kesalahan dan kelalaian, dapat diupayakan beberapa konsep berikut:

1. ***Least privilege***. Jika hak akses hanya diberikan kepada sedikit orang, dapat mengurangi kemungkinan terjadinya kesalahan dan kelalaian.

2. ***Backups of the information on the systems***. Saat terjadi kehilangan integritas dari sistem informasi, mudah untuk menelusuri kembali informasi yang benar dari backup-nya. Backup data merupakan tool yang penting bagi seorang manajer keamanan informasi dan seringkali menjadi satu-satunya jalan menanggulangi dampak dari serangan.

# 3. Fraud and Theft (penipuan dan pencurian)


- Jika pengguna akhir bukan secara tidak sengaja menghancurkan data tetapi secara jahat merusak informasi tersebut, berarti kita menghadapi masalah yang berbeda.
- Bagi sebagian besar karyawan, sulit membayangkan bahwa rekan kerja datang ke kantor setiap hari dengan niat buruk, tetapi hal tersebut dapat saja terjadi.
- Cara terbaik melawan penipuan dan pencurian adalah dengan menggunakan kebijakan yang tegas. Kebijakan yang dapat membuat manajer keamanan informasi mudah dalam mengumpulkan fakta untuk membuktikan aksi jahat yang dilakukan oleh karyawan.

# 3. Fraud and Theft

- Jika dalam organisasi sudah ada kebijakan yang tegas, manajer keamanan informasi dapat menggunakan teknik forensik untuk mengumpulkan bukti yang membantu mencari informasi seputar pelaku kejahatan.
- **Pertama: "do no harm".** Hal ini berarti jika kita tidak yakin apa yang harus dilakukan, maka jangan melakukan apapun terhadap sistem. Setiap kali professional teknis menggerakan mouse atau menyentuh keyboard untuk memasukkan perintah, sistem berubah. Hal ini dapat membuat bukti yang dikumpulkan dari sistem menjadi lebih susah.
- Terdapat banyak tempat yang membuktikan aktifitas yang ditinggalkan (firewall, server logs, client workstation, dsb), merupakan tempat-tempat yang harus diselidiki untuk menentukan apakah ada bukti lain yang tersisa.

# 3. Fraud and Theft

- **Tahap kedua**, yaitu: **"pull the plug"**. Tetapi resikonya jika sistem kita memiliki hard drive terenkripsi, kita mungkin tidak akan pernah bisa mengetahui informasi apa yang ada di sistem itu.
- Setelah professional mendapatkan sistem yang dicurigai (atau minimal hard drive-nya), dia akan membuat sebuah bit-stream backup dari hard drive tersebut. Setelah copy dibuat, dilakukan pembandingan dari hard drive copy dan hard drive backup menggunakan teknologi yang dinamakan MD5 hash*. Sehingga dapat diketahui apakah data yang didapatkan dari kedua driver tsb sama atau tidak.

*Dibahas di mata kuliah Kriptografi

# 4. Malicious Hackers

- Definisi hacker menurut Guy L. Steele:

  "Seseorang yang merupakan musuh dari pengguna komputer yang sangat senang belajar komputer dan ahli dalam bahasa pemrogramannya kemudian senang membanggakan diri dalam menunjukkan kemampuan mereka dengan meretas sistem orang lain" (Guy L. Steele, Hacker's Dictionary)

- Terdapat beberapa hal yang menyebabkan pesatnya pertumbuhan hacker dunia termasuk Indonesia. Beberapa penyebab ini sulit diantisipasi namun perlu disikapi secara positif oleh kompenen negara terkait.

- Penyebab maraknya hacker di Indonesia:
  1. Buku panduan yang banyak beredar
  2. Fasilitas internet semakin murah

# 4. Malicious Hackers

- Tipe hacker dilihat dari sisi motivasi kegiatan mereka:

1. ***Black hat***, melakukan tindakan destruktif terhadap sistem komputer untuk mendapatkan imbalan.
2. ***White hat***, menjaga keamanan dari serangan untuk melindungi sistem komputer.
3. ***Gray hat***, terkadang melakukan tindakan offensive, terkadang melakukan tindakan defensive.
4. ***Suicide hat***, melakukan tindakan peretasan dengan visi utama meretas objek-objek vital sebuah negara, tanpa takut terhadap hukum.
5. ***Blue hat***, seorang praktisi keamanan sistem informasi yang aktif mengajarkan kemampuannya dalam peretasan maupun pertahanan sistem kepada orang lain.

# 4. Malicious Hackers

- Beberapa alasan hacker beroperasi:

  1. ***Thriil seeker***, hanya untuk mencari sensasi dan kepuasan diri.

  2. ***Organized crime***, didanai oleh pihak tertentu untuk sebuah misi tertentu. Seperti pencucian uang, pembodohan publik, pembunuhan karakter, dsb.

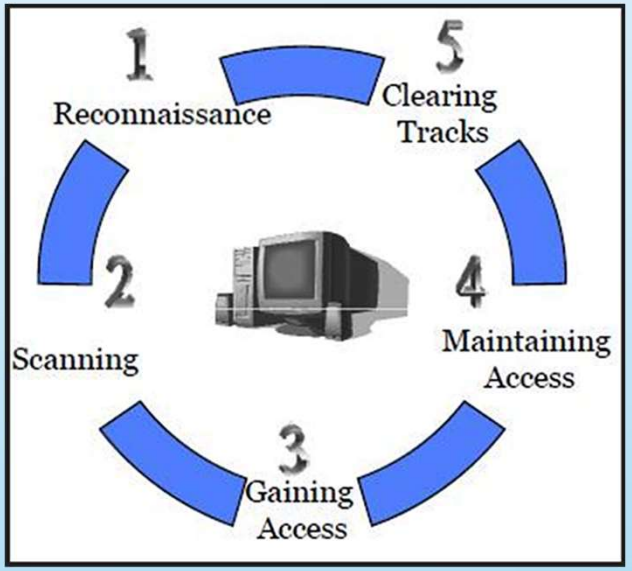
  3. ***Terorist group***, hadir di belahan dunia untuk tujuan yang lebih besar. Dimulai dari perekrutan anggota, pencucian otak, sampai peretasan jaringan infrastruktur suatu negara seperti fasilitas listrik, telekomunikasi, jaringan perbankan, dsb.

  4. ***Intelligent***, membantu melakukan kegiatan intelijen demi keutuhan sebuah negara.

* Pintar dan baik adalah dua hal yang berbeda.

# 4. Malicious Hackers

- Lima langkah hacker beroperasi:




1. ***Reconnaisance***, tahap pengumpulan informasi.
2. ***Scanning***, mencari celah keamanan infrastruktur target.
3. ***Gaining access***, melakukan peretasan.
4. ***Maintaining access***, menjaga dan merawat akses jalan masuk.
5. ***Clearing track***, menghilangkan atau menghapus jejak.

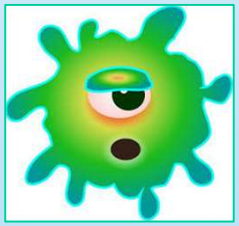
# 4. Malicious Hackers

Beberapa istilah lain:

- ***Cracker***, beberapa pendapat mengatakan bahwa cracker mempunyai definisi yang sama dengan hacker tetapi berbeda dalam hal aktifitasnya saja.
- ***Phreaker***, hampir sama dengan cracker namun lebih memfokuskan dirinya pada bugs dalam sebuah sistem jaringan telekomunikasi. Ada juga yang mengatakan bahwa phreaker singkatan dari PHone fREe And hacKER (http://waparea.com.nu)
- ***Defacer***, fokus pada kegiatan mengubah tampilan suatu website.
- dsb.

# 5. Malicious Code

- Terdapat banyak tipe berbeda dari *malicious code* (kode perusak). Empat yang umum di antaranya adalah virus, worm, trojan horse, logic bom, dsb.



***Viruses***. Sebuah program yang "menyimpang", tersimpan di media penyimpanan, yang dapat menyebabkan hal-hal yg tidak terduga atau diinginkan, misalnya merusak / menghapus data.

***Worms***. Program bersifat merusak yang dapat menyalin dirinya sendiri tanpa memerlukan program lain ke memori atau peralatan penyimpan.

***Trojan horses***. Program yang bersembunyi di program yang lain, dan menampakkan perilaku sesuai rancangannya hanya apabila diaktifkan.

**Logic bombs**. Dirancang untuk diaktifkan dan mengerjakan suatu aksi yang merusak pada waktu tertentu.

# 6. Denial-of-Service Attacks

- Sebagai penyerang, jika Anda tidak bisa mendapatkan akses ke jaringan target, bisa jadi hal terbaik yang dapat Anda lakukan adalah memastikan bahwa tidak boleh ada yang mendapatkan akses ke jaringan tersebut.
- Hal di atas dilakukan dengan memberikan serangan DoS, yang dirancang untuk membanjiri sumber daya perangkat keras server atau membanjiri jalur telekomunikasi jaringan target. Selama bertahun-tahun terdapat sejumlah serangan DoS “one-to-one”, yang menyerang dari sistem ke server target atau jaringan.
- Contoh dari jenis serangan tersebut adalah *Syn floods*, *Fin floods*, *Smurfs*, dan *Fraggles*.
- Pada Feb 2000, DoS menyerang dengan cara lebih canggih. Saat itu, sejumlah target diambil alih oleh serangan next generation of DoS (the distributed DoS / DDoS). DDoS tidak menyerang menggunakan “one-to-one” lagi, tetapi menggunakan host zombie untuk menciptakan serangan “many-to-one”.

# 7. Social Engineering

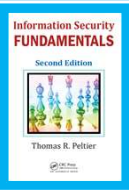
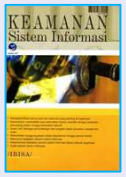
- *Social engineering* merupakan nama yang diberikan untuk kategori serangan keamanan dimana seseorang memanipulasi orang lain untuk memberikan informasi yang dapat digunakan untuk mencuri data, akses ke sistem, akses ke ponsel, uang, atau bahkan identitas pribadi.
- Saat ini, mendapatkan akses informasi melalui telepon atau melalui situs web yang Anda kunjungi, dapat menjadi sarana baru bagi penjahat jenis ini.
- Tujuan dari social engineering adalah untuk mengelabui seseorang agar memberikan informasi berharga atau akses ke informasi / sumber daya tersebut. Penjahat kategori ini memangsa orang yang memiliki sifat:
  - ✓ Keinginan kuat untuk membantu
  - ✓ Kecenderungan mudah untuk mempercayai orang
  - ✓ Takut mendapat masalah
  - ✓ Kesediaan untuk mengambil jalan pintas.

# 7. Social Engineering

- Berdasarkan Jargon Dictionary, "*Wetware*" adalah sifat manusiawi yang melekat pada sistem. Manusia biasanya merupakan elemen terlemah dalam rantai keamanan.
  - *"In the 1970s, we were told that if we installed access control packages, we would have security.*
  - *In the 1980s, we were encouraged to install effective antivirus software to ensure that our systems and networks were secure.*
  - *In the 1990s, we were told that firewalls would lead us to security.*
  - *Now in the 21st century, it is intrusion detection systems or public key infrastructure that will lead us to information security".*
- Pada setiap tahap perkembangan komputer, keamanan selalu luput dari kita karena *silicon-based products* harus berhadapan dengan *carbon-based unit* (faktor manusiawi).

# Referensi

Thank's to:


| | |
|---|---|
|  | Thomas R. Peltier, Justin Peltier, John Blackley. **Information Security Fundamentals.** CRC Press. 2005 (2nd Edition, 2014). |
|  | Yurindra, M.T **Keamanan Sistem Informasi.** Deepublish. 2014. |
|  | IBISA **Keamanan Sistem Informasi.** Penerbit Andi. 2011. |

# Diskusi

- Temukan contoh kasus dari ancaman organisasi terkait dengan informasi yang dapat disebabkan oleh:
  1. Kegagalan perangkat keras
  2. Kegagalan perangkat lunak
  3. Kegagalan SDM
  4. Alam
  5. Keuangan
  6. Eksternal
  7. Internal
- Jelaskan penyebab, akibat, dan cara menanggulanginya!

# End of File