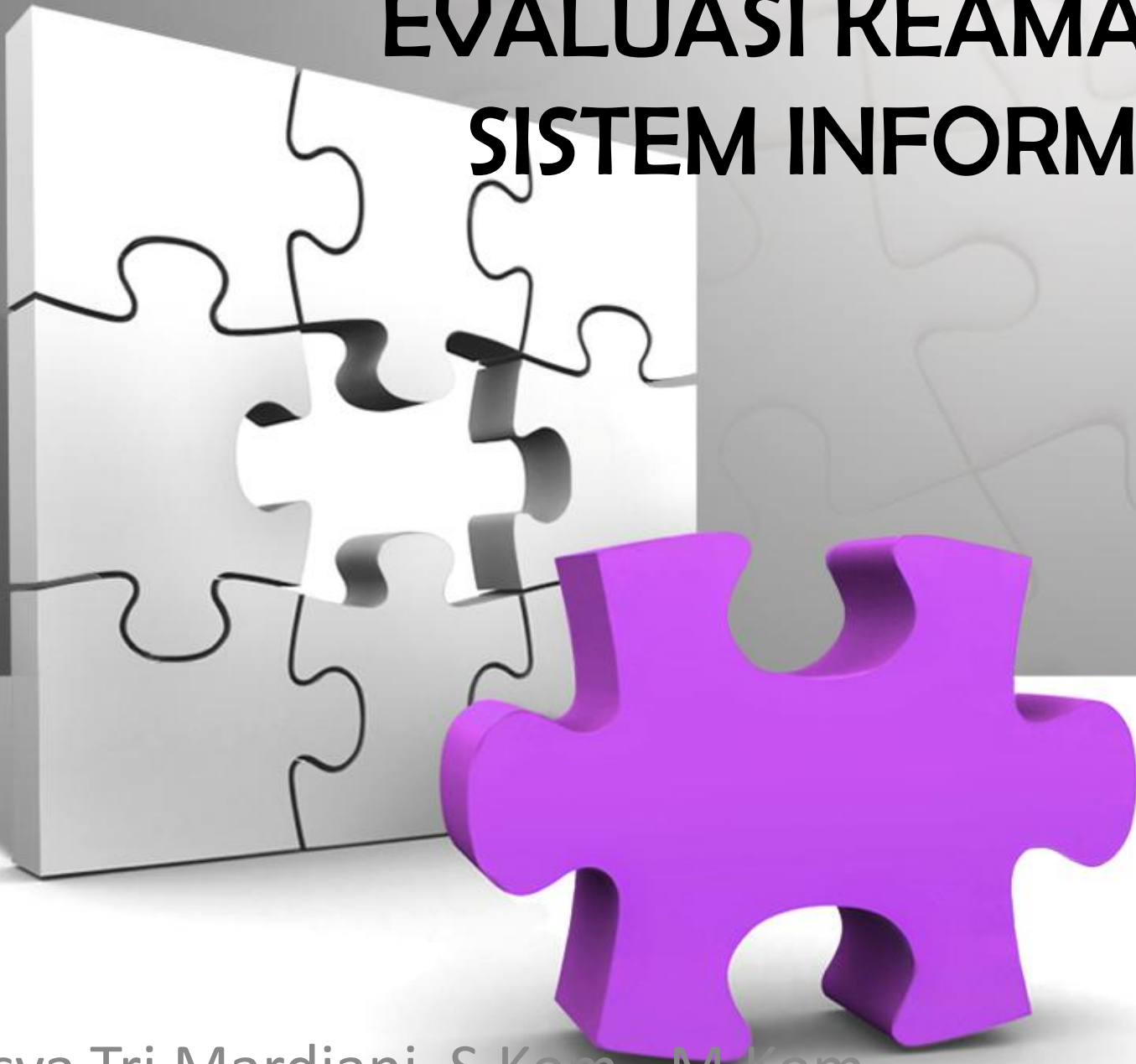


# EVALUASI KEAMANAN SISTEM INFORMASI



Gentisya Tri Mardiani, S.Kom., M.Kom

# Pendahuluan




- Kriteria dalam masalah keamanan yang harus diperhatikan:
  1. Akses kontrol sistem yang digunakan
  2. Telekomunikasi dan jaringan yang dipakai
  3. Pengembangan sistem aplikasi yang digunakan
  4. Cryptography yang diterapkan
  5. Arsitektur dari sistem informasi yang diterapkan
  6. Pengoperasian dan tata letak fisik dari sistem yang ada
  7. Risk Management, Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
  8. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan



# Faktor evaluasi keamanan

- Lubang keamanan (security hole)
- Kesalahan konfigurasi
- Penambahan perangkat baru (hardware/  
software)



# Sumber Lubang Keamanan

- Kesalahan desain (*desain flaw*)
- Implementasi kurang baik
- Kesalahan konfigurasi
- Kesalahan menggunakan program atau sistem



# PENGENDALIAN KEAMANAN SISTEM INFORMASI

Berkaitan dengan masalah keamanan sistem informasi, diperlukan tindakan berupa pengendalian terhadap sistem informasi.

Kontrol-kontrol untuk pengamanan sistem informasi antara lain:

- a) Kontrol Administratif
- b) Kontrol Pengembangan dan Pemeliharaan Sistem
- c) Kontrol Operasi
- d) Proteksi Fisik terhadap Pusat Data



# PENGENDALIAN KEAMANAN SISTEM INFORMASI

Kontrol-kontrol untuk pengamanan sistem informasi antara lain:

- e) Kontrol Perangkat Keras
- f) Kontrol Akses terhadap Sistem computer
- g) Kontrol terhadap Akses Informasi
- h) Kontrol terhadap Bencana
- i) Kontrol terhadap Perlindungan Terakhir
- j) Kontrol Aplikasi

# Kontrol Administratif



Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka kontrol dilaksanakan sepenuhnya dalam organisasi berdasarkan prosedur-prosedur yang jelas.

# Kontrol Administratif



Kontrol ini mencakup hal-hal berikut:

1. Mempublikasikan kebijakan control yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi.
2. Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk proses pengembangan sistem, prosedur untuk *backup*, pemulihan data, dan manajemen pengarsipan data.
3. Perekrutan pegawai secara berhati-hati yang diikuti dengan orientasi pembinaan, dan pelatihan yang diperlukan.



# Kontrol Administratif



4. Supervisi terhadap para pegawai. Termasuk pula cara melakukan control kalau pegawai melakukan penyimpangan terhadap yang diharapkan.
5. Pemisahan tugas-tugas dalam pekerjaan dengan tujuan agar tak seorangpun yang dapat menguasai suatu proses yang lengkap.



# Kontrol Pengembangan dan Pemeliharaan Sistem

- Peran auditor sistem informasi sangatlah penting.
- Auditor sistem informasi harus dilibatkan dari masa pengembangan hingga pemeliharaan system, untuk memastikan bahwa sistem benar-benar terkendali, termasuk dalam hal otorisasi pemakai sistem.




# Kontrol Operasi

Kontrol operasi dimaksudkan agar sistem beroperasi sesuai dengan yang diharapkan. Hal – hal yang termasuk dalam kontrol ini:

- Pembatasan akan akses terhadap data
- Kontrol terhadap personel pengoperasian
- Kontrol terhadap peralatan
- Kontrol terhadap penyimpanan arsip
- Pengendalian terhadap virus

Untuk mengurangi terjangkitnya virus, administrator sistem harus melakukan tiga kontrol berupa preventif, detektif, dan korektif.

<b>Kontrol</b>	<b>Contoh</b>
<b>Preventif</b>	<ul style="list-style-type: none"> <li>○ <b>Menggunakan salinan perangkat lunak atau berkas yang berisi makro yang benar-benar bersih.</b></li> <li>○ <b>Mengindari pemakaian perangkat lunak <i>freeware</i> atau <i>shareware</i> dari sumber yang belum bisa dipercaya.</b></li> <li>○ <b>Menghindari pengambilan berkas yang mengandung makro dari sembarang tempat.</b></li> <li>○ <b>Memeriksa program baru atau berkas-berkas baru yang mengandung makro dengan program anti virus sebelum dipakai.</b></li> <li>○ <b>Menyadarkan pada setiap pemakai untuk waspada terhadap virus.</b></li> </ul>
<b>Detektif</b>	<ul style="list-style-type: none"> <li>○ <b>Secara rutin menjalankan program antivirus untuk mendeteksi infeksi virus.</b></li> <li>○ <b>Melakukan perbandingan ukuran-ukuran berkas untuk mendeteksi perubahan ukuran pada berkas</b></li> <li>○ <b>Melakukan perbandingan tanggal berkas untuk mendeteksi perubahan tanggal berkas.</b></li> </ul>
<b>Korektif</b>	<ul style="list-style-type: none"> <li>○ <b>Memastikan pem-<i>backup</i>-an yang bersih</b></li> <li>○ <b>Memiliki rencana terdokumentasi tentang pemulihan infeksi virus.</b></li> <li>○ <b>Menjalankan program antivirus untuk menghilangkan virus dan program yang tertular.</b></li> </ul>



# Proteksi Fisik terhadap Pusat Data

- Pusat data merupakan aset bagi sistem informasi
- Menjaga hal-hal yang tidak diinginkan terhadap pusat data.
- Faktor lingkungan seperti suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar.



# Kontrol Perangkat Keras

- Mengantisipasi kegagalan sistem komputer, organisasi menerapkan sistem komputer yang berbasis *fault-tolerant* (toleran terhadap kegagalan).
- Pada sistem ini, jika komponen dalam sistem mengalami kegagalan maka komponen cadangan segera mengambil alih peran komponen yang rusak



# Kontrol Perangkat Keras

Sistem *fault-tolerant* dapat diterapkan pada lima level, yaitu:

No	Level	Action
1	Komunikasi Jaringan	Toleransi kegagalan terhadap jaringan dilakukan dengan menduplikasi jalur komunikasi dan processor
2	Processor	Redundansi prosesor dilakukan antara lain dengan teknik <i>watchdog processor</i> , yang akan mengambil alih prosesor yang bermasalah
3	Penyimpanan Eksternal	Melalui <i>disk mirroring</i> atau <i>disk shadowing</i> , yang menggunakan teknik dengan menulis seluruh data ke dua <i>disk</i> secara paralel
4	Catu Daya	Toleransi kegagalan pada catu daya diatasi melalui UPS
5	Transaksi	Ditangani melalui mekanisme <i>rollback</i> , yang akan mengembalikan ke keadaan semula yaitu keadaan seperti sebelum transaksi dimulai sekiranya di pertengahan pemrosesan transaksi terjadi kegagalan



# Kontrol Akses terhadap Sistem Komputer

- untuk melakukan pembatasan akses terhadap sistem, setiap pemakai sistem diberi otorisasi yang berbeda-beda, dilengkapi dengan username dan *password*.
- dapat dilakukan dengan mengkombinasikan teknologi lain. Misalnya, smartcard untuk mengakses sistem dengan pemasukan PIN (*personal identification number*).
- akses Intranet dari pemakai luar (via Internet) dapat dicegah dengan menggunakan *firewall*.



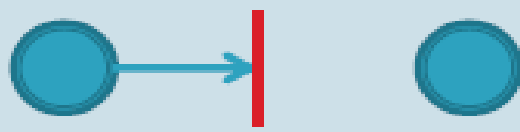
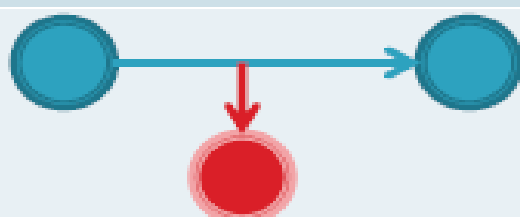
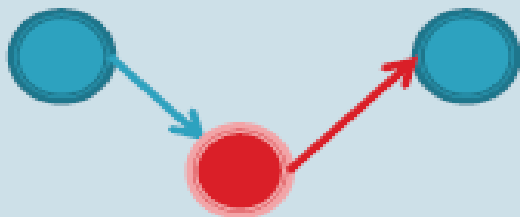
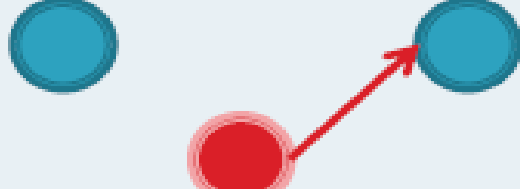


# Kontrol Akses Informasi

- Mencegah kemungkinan keberhasilan pihak yang tidak berwenang mengakses dan membaca informasi melalui jaringan
- Perlu dilakukan penyandian informasi untuk mencegah penyadapan informasi, dengan kriptografi.

# Kontrol Akses Informasi

Jenis ancaman yang perlu diperhatikan:

Ancaman	Contoh	Ilustrasi
Interruption	Perusakan HDD, pemotongan jalur komunikasi	
Interception	Penyadapan data melalui jaringan publik (wiretapping)	
Modification	Melakukan perubahan program, menyisipkan malicious code	
Fabrication	Menambahkan record ke basis data	



# Kontrol Terhadap Bencana

Rencana pemulihan terhadap bencana ke dalam 4 komponen:

- Rencana darurat (*emergency plan*) menentukan tindakan-tindakan yang harus dilakukan oleh para pegawai ketika bencana terjadi.
- Rencana cadangan (*backup plan*) menentukan bagaimana pemrosesan informasi akan dilaksanakan selama masa darurat.



# Kontrol Terhadap Bencana

- Rencana pemulihan (*recovery plan*) menentukan bagaimana pemrosesan akan dikembalikan ke keadaan seperti aslinya secara lengkap, termasuk mencakup tanggung jawab masing-masing personil.
- Rencana pengujian (*test plan*) menentukan bagaimana komponen-komponen dalam rencana pemulihan akan diuji atau disimulasikan



# Kontrol Terhadap Perlindungan Terakhir

Kontrol terhadap perlindungan terakhir dapat berupa:

- Rencana pemulihan terhadap bencana.
- Asuransi.

Asuransi merupakan upaya untuk mengurangi kerugian sekiranya terjadi bencana. Itulah sebabnya, biasanya organisasi mengansuraskan gedung atau asset-aset tertentu dengan tujuan kalau bencana terjadi, klaim asuransi dapat digunakan untuk meringankan beban organisasi



# Kontrol Aplikasi

Kontrol aplikasi adalah kontrol yang diwujudkan secara spesifik dalam suatu aplikasi sistem informasi. Wilayah yang dicakup oleh kontrol ini meliputi:

- Kontrol Masukan
- Kontrol Pemrosesan
- Kontrol Keluaran
- Kontrol Basis Data
- Kontrol Telekomunikasi



# PENGUJI KEAMANAN SISTEM

- Dikarenakan banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan “*automated tools*”, perangkat pembantu otomatis, yang dapat membantu menguji atau mengevaluasi keamanan sistem yang dikelola.



# PENGUJI KEAMANAN SISTEM

- Untuk sistem yang berbasis UNIX ada beberapa tools yang dapat digunakan, yaitu:
  - *Cops*
  - *Tripwire*
  - *Satan/Saint*
  - *SBSscan: localhost security scanner*
- Untuk sistem yang berbasis Windows NT ada juga program semacam, misalnya program *Ballista* yang dapat diperoleh dari:  
<<http://www.secnet.com>>





# PENGUJI KEAMANAN SISTEM

Program yang digunakan untuk menguji keamanan sistem, seperti:

- Crack
- *Land* dan *Latierra*
- *ping-o-death*
- *winnuke*



# Probing Services

- Melihat servis yang diberikan oleh server.
- Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:
  - SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
  - POP3, untuk mengambil e-mail, TCP, port 110



- **Paket probe untuk sistem UNIX**
  - *nmap*
  - *strobe*
  - *tcpprobe*
- **Probe untuk sistem Window 95/98/NT**
  - *NetLab*
  - *Cyberkit*
  - *Ogre*





# TUGAS KELOMPOK

- Cari informasi, mengenai:
  - Definisi, sejarah,
  - Tujuan/ fungsi penggunaan,
  - Fitur,
  - Kelebihan dan kekurangan,
  - Contoh aplikasi, penerapan aplikasi
  - Kesimpulan

Dikumpulkan makalah (hardcopy) dan presentasi kelompok minggu depan.



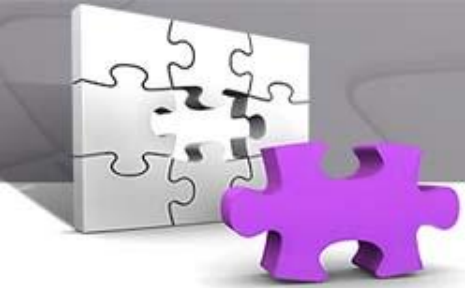
# TUGAS KELOMPOK

Materi yang dibahas:

1. Tripwire
2. Program crack
3. WinNuke
4. Nmap
5. Strobe
6. Snort
7. Wireshark
8. Cyberkit

Ketentuan makalah:

- Cover
- Daftar isi
- Isi
- Kesimpulan
- Referensi



See u next week..