

Physical Security





Definisi Physical Security



Tindakan atau cara yang dilakukan untuk mencegah atau menanggulangi dan menjaga hardware, program, jaringan dan data dari bahaya fisik dan kejadian yang dapat menyebabkan kehilangan yang besar atau kehancuran. Keamanan fisik termasuk perlindungan terhadap kebakaran, bencana alam, pencurian, vandalism dan teroris

Yang perlu dilindungi adalah:

- Bangunan
- Ruang Komputer
- Komputer
- Media Penyimpanan





Lingkungan

- Kebakaran
- Iklim
- Gempa Bumi dan Getaran
- Air
- Listrik
- Petir

Orang

Dilindungi Terhadap
Apa?

CYBER SECURITY



Physical

Security

Awalnya dianggap tidak penting

Sering diabaikan

Karena sering banyak kejadian, seperti

- pencurian fisik : laptop, hardisk, CD

- Bencana Alam

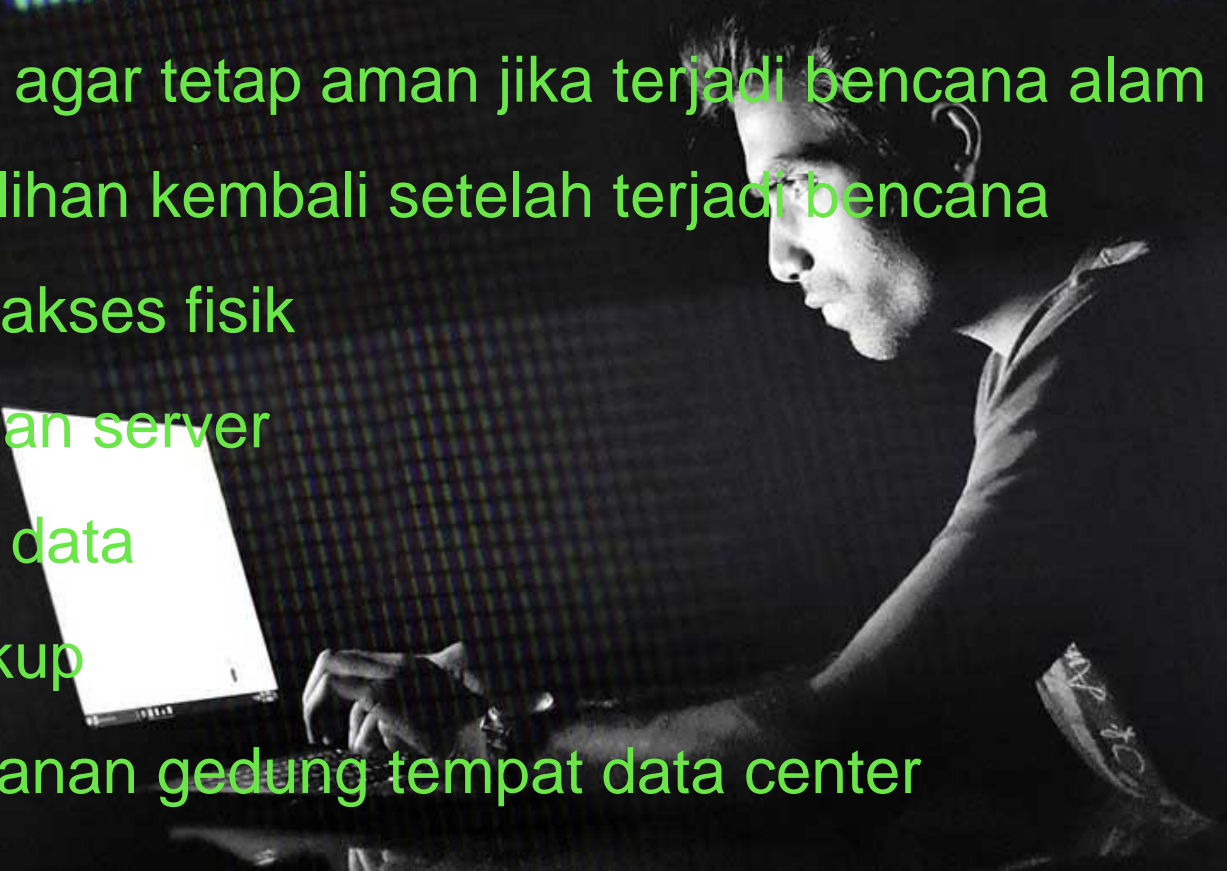
Kebijakan keamanan fisik mulai diperhatikan,
dilihat ulang dan diperbaiki



Physical

Security

- ❖ Bagaimana menjaga data agar tetap aman jika terjadi bencana alam
- ❖ Bagaimana strategi pemulihan kembali setelah terjadi bencana
- ❖ Bagaimana pengontrolan akses fisik
- ❖ Bagaimana standar ruangan server
- ❖ Bagaimana penyimpanan data
- ❖ Bagaimana prosedur backup
- ❖ Bagaimana standar keamanan gedung tempat data center



Ancaman dan resiko pada data center



Faktor lingkungan

- kebakaran, banjir, embun, suhu, listrik, gempa bumi dan bentuk-bentuk bencana alam lainnya
- Faktor manusia
- eksploitasi
- Faktor finansial
- butuh investasi yang cukup lumayan



Metode pengamanan Fisik pada data center



Faktor lingkungan – Bangunan(Lokasi)

Lokasi data center dipilih yang memiliki sedikit resiko terhadap bencana alam dan ancaman teroris
Sebaiknya terpisah dengan kantor pusat

Jauh dari jalan raya utama

Lokasi tidak bertetangga dengan bandar udara, pabrik kimia, jalur pipa gas, pusat keramaian dan pusat pembangkit listrik

Memiliki kecukupan tenaga listrik



Metode pengamanan Fisik pada data center



Faktor lingkungan – Bangunan (kontruksi bangunan)

- Perhatikan mengenai sirkulasi udara, terkait dengan suhu. Kebanyakan sedikit jendela dan tertutup.
- Gunakan standar pendingin ruangan
- Bahan bangunan tidak mudah terbakar
- Kontruksi bangunan tahan gempa
- Instalasi listrik yang baik, terutama grounding
- Pintu masuk dirancang sangat terbatas
- Pintu kebakaran dirancang untuk keluar saja



Metode pengamanan Fisik pada data center



Faktor lingkungan – Bangunan (pengamanan di sekeliling bangunan)

- Memiliki jarak +/- 10 meter dari bangunan lain/pohon
- Gunakan CCTV untuk pengawasan di sekitar bangunan
- Perlu pepohonan dan taman agar tersembunyi dari orang lewat dan pengintai
- Area parkir kendaraan perlu diawasi, gunakan petugas yang profesional dan detektor bom

Metode pengamanan Fisik pada data center



Faktor lingkungan – Bangunan (pengamanan di dalam bangunan)

- Perlu kamera pengawas, sensor asap, sensor kebakaran.
- Pengawasan terhadap pintu masuk dan keluar



Metode pengamanan Fisik pada data center



Faktor lingkungan – Kebakaran

Suplai listrik yang baik perlu diperhatikan

Bangunan tidak mudah terbakar

Gunakan sensor asap, sensor panas, pemadam api dan sistem penyemprot air.

Periksa secara periodik

Gunakan alarm kebakaran baik yang manual maupun yang otomatis

Perlu kebijakan dilarang merokok di ruang komputer



Metode pengamanan Fisik pada data center



Faktor lingkungan – Suhu/Iklim

- Perlu sensor suhu di ruang server
- Gunakan AC yang cukup untuk membuat ruangan tetap dingin
- Suhu yang baik 10-26 derajat Celcius
- Kelembaban antara 20-80 persen
- Gunakan alarm bila melebihi batas suhu dan kelembaban
- Pendingin dan pemanas perlu diberi filter untuk menghindari debu



Metode pengamanan Fisik pada data center



Faktor lingkungan – Listrik

- Voltase dan daya harus cukup
- Grounding yang baik
- Perlu stabiliser
- Perlu listrik cadangan, seperti UPS dan Genset



Metode pengamanan Fisik pada data center



Faktor lingkungan – Bencana alam

- ❖ Bangunan harus jauh dari daerah yang sering dilanda bencana alam.
- ❖ Kontruksi bangunan harus tahan gempa
- ❖ Pastikan kalau terjadi gempa yang kuat, tidak ada benda-benda yang jatuh menimpa komputer.
- ❖ B A C K U P !!
- ❖ Penyimpanan hasil data backup perlu diperhatikan
- ❖ Harus aman dari penyusup, ruangan harus baik, bebas debu, tidak lembab dan tidak mudah terbakar

Metode pengamanan Fisik pada data center



Faktor lingkungan – Air

- Banjir dapat terjadi karena hujan, air dari kamar mandi meluap, dari sprinklers. Pastikan terhindar dari semuanya itu
- Bila komputer terlanjur basah, keringkan dahulu sebelum dinyalakan
- Gunakan sensor air di lantai dekat komputer.



Metode pengamanan Fisik pada data center



Faktor lingkungan – Petir

Gunakan penangkal petir yang baik

Kabel penangkal petir harus sampai mencapai air tanah

Bila terjadi petir yang sering, matikan komputer dan lepaskan kabel-kabel, seperti kabel listrik, kabel jaringan.

- ## Faktor Manusia

- Sering kali eksploitasi dilakukan oleh orang dalam
- Digunakan teknologi biometric
- Biasanya digunakan sebagai otentikasi untuk masuk ke ruangan khusus, seperti ruang server, ruang komputer atau untuk mengakses suatu sistem

Biometrics



Dapat berupa:

sidik jari, telapak tangan, pola retina, pola suara, tanda tangan dan pola mengetik.



Biometrics



SIDIK JARI

Setiap manusia memiliki sidik jari yang unik

Pemeriksaan pada pola dari minutiae

Sebuah jari memiliki minutiae sampai 150

Kelemahan: luka bakar dan luka fisik pada jari

debu, keringat, minyak dan lem pada jari bisa mempengaruhi



Biometrics



TELAPAK TANGAN

Setiap manusia memiliki pola telapak tangan yang unik

Pemeriksaan dilakukan pada guratan tangan

Luka, bengkak dan pemakaian cincin pada tangan dapat mempengaruhi sistem ini



Biometrics



POLA RETINA

Setiap manusia memiliki pola retina yang unik

Menggunakan sinar infra merah

Pengukuran dilakukan intensitas cahaya dari pembuluh darah pada retina

Sangat terpercaya, tetapi kurang diterima

Ditakutkan membutakan mata



Biometrics



POLA SUARA

Setiap manusia memiliki pola suara dan akustik yang unik

Suara dikonversi ke bentuk digital lalu dibandingkan dengan pola yang sudah tersimpan

Penyakit pernapasan, luka, stress dan gangguan dari suara latar belakang dapat mempengaruhi sistem ini



Biometrics



POLA TANDATANGAN

Setiap manusia memiliki pola tandatangan yang unik

Menggunakan pad dan pen biometric yang dihubungkan ke komputer

Tandatangan dikonversi ke dalam bentuk signal digital

Tekanan pen pada saat tandatangan dapat mempengaruhi bentuk signal digital



Biometrics



POLA KETIKAN

Setiap manusia memiliki pola atau ritme mengetik

Sistem memberikan sebuah kalimat untuk kita ketik

Pola dan ritme mengetik yang kita lakukan akan dibandingkan dengan pola yang telah tersimpan.





THANK YOU

Computer Security