Chapter #5
Keamanan Fisik

AIK21363 (3 sks)

Keamanan dan Jaminan Informasi
Information Assurance and Security

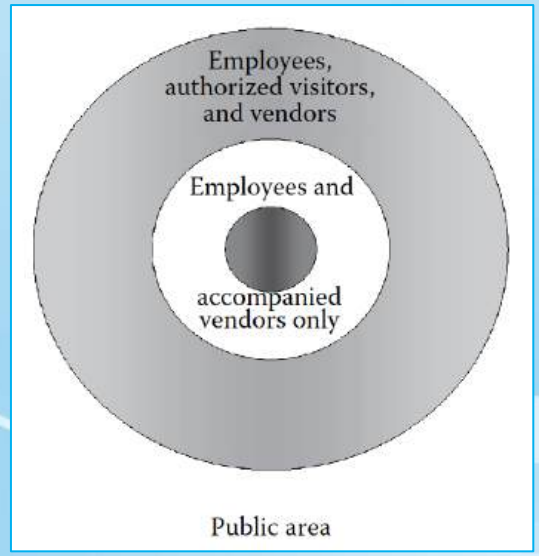
Nurdin Bahtiar, M.T
Prajanto Wahyu Adi, M.Kom

Materi

1. Data Centre Requirements
2. Physical Access Controls
3. Fire Prevention and Detection
4. Intrusion Detection Systems
5. Sample Physical Security Policy
6. Sample Data Centre Infrastructure
7. Summary

1. Data Center Requirements

- Sifat keamanan secara fisik terhadap pusat data seharusnya merupakan cincin pertahanan terpusat - dimana persyaratan untuk masuknya semakin dekat ke pusat cincin semakin sulit.
- Meskipun karyawan perusahaan, pengunjung resmi, dan vendor diizinkan berada dalam lingkaran luar, hanya karyawan pusat data dan vendor yang menyertainya saja yang boleh berada di dalam lingkaran dalam.



1. Data Center Requirements

- Alasannya jelas, jika kita mengambil sejumlah tindakan pencegahan untuk melindungi informasi yang diakses banyak orang, setidaknya harus dipastikan bahwa tidak ada kerusakan atau gangguan yang terjadi pada perangkat kerasnya.

- Lebih jauh, fisik pusat data juga harus dipertimbangkan. Apakah bangunannya khusus berdiri sendiri atau berada dalam gedung yang menampung fungsi lainnya? Jika berada di gedung khusus, hal terbuka apa yang terkait gedung tersebut dan bagaimana perlindungan staf saat mereka masuk / keluar gedung?

1. Data Center Requirements

- Selanjutnya, prinsip konsistensi harus tetap diterapkan. Buat apa membangun kontrol akses fisik dengan biaya beberapa juta dolar jika potensi kerusakan yang dapat dilakukan pada pusat data kurang dari beberapa puluh juta dolar.
- Ingatlah, bahwa biaya pengontrolan tersebut memiliki konsistensi terhadap nilai asset yang dilindungi, serta definisi 'konsisten' tersebut bergantung pada resiko organisasi yang disepakati oleh pihak manajemen.

1. Data Center Requirements

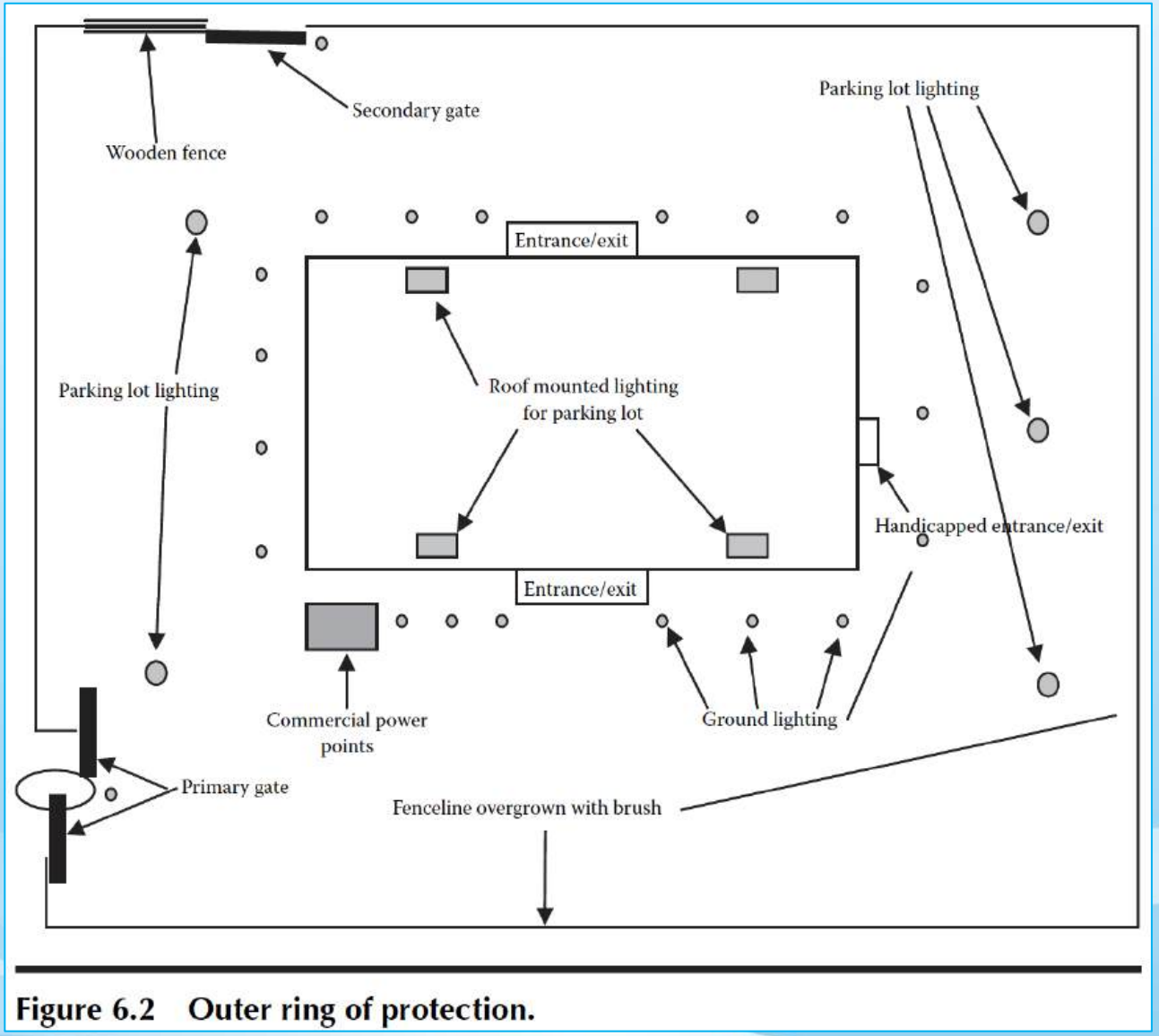


Figure 6.2 Outer ring of protection.

2. Physical Access Controls

Aset yang akan Dilindungi

- Beberapa instansi bisa jadi memutuskan untuk memusatkan operasi dengan membangun “ruang server” yang besar dan mahal di lokasi mereka. Alternatif lain, instansi mungkin memutuskan untuk mengambil pendekatan desentralisasi dan mendistribusikan komputer dan peralatan komputasi di sekitar gedung-gedung yang ada.

- Jumlah upaya yang dilakukan untuk melindungi aset fisik pada kedua skenario di atas bisa jadi sama, tetapi akan memiliki bentuk perlindungannya akan berbeda.

- Untuk server besar, beberapa perlindungan cincin pertahanan terpusat berbasis teknologi dan kontrol akses mungkin sesuai. Sedangkan untuk versi terdistribusi, cukup menyimpan server individual di ruang terkunci mungkin cukup. Hal ini merupakan salah satu variasi yang harus dipertimbangkan ketika memilih kontrol akses fisik yang tepat.

2. Physical Access Controls

Potensi Ancaman

- Ketika menilai potensi ancaman, dosis besar akal sehat merupakan alat terbaik. Ancaman yang ada untuk operasi komersial tingkat tinggi atau sensitif politik sangat berbeda dari yang dihadapi (misalnya) produsen biskuit. Demikian juga, pusat operasi yang terletak di tengah-tengah kota yang bergejolak akan menghadapi ancaman yang jauh lebih besar daripada yang berlokasi di taman industri dekat perkampungan.

- Sifat dan sejarah organisasi terkini juga harus diperhitungkan. Misalnya, jika organisasinya stabil dan telah lama berdiri tanpa ada riwayat perselisihan karyawan, maka tindakan pencegahan ancaman (dalam bentuk langkah-langkah keamanan fisik) yang akan diambil akan jauh lebih sedikit daripada jika organisasi memiliki reputasi karyawan yang tidak puas dan aktivitas yang mengganggu di lokasi. Hal ini adalah variasi kedua yang harus dipertimbangkan ketika memilih kontrol akses fisik.

3. Fire Prevention and Detection

Fire Prevention

- "Dilarang merokok" adalah aturan pertama. Meskipun ini merupakan persyaratan umum di seluruh negara, namun, penggunaan bahan rokok di mana saja di dalam gedung pusat informasi penting harus dilarang.
- Semua bahan yang mudah terbakar (seperti kertas printer, pembungkus plastik, dsb) harus disimpan di area yang terpisah dari server utama atau ruang komputer dengan dinding yang tahan api. Persediaan untuk pemrosesan 1 hari dapat disimpan di server atau ruang komputer tetapi persediaan yang lebih besar harus disimpan secara terpisah.

3. Fire Prevention and Detection

Fire Detection

- Sumber kebakaran paling umum adalah sistem listrik atau perangkat keras. Kerusakan pada isolasi dan hubungan arus pendek yang dihasilkan dapat menyebabkan panas yang hebat yang dapat melelehkan bahan atau menyebabkan kebakaran.
- Kebakaran di pusat data sering kali kecil, akibat sedikit efek pada suhu dingin di dalam ruangan. Karena asap itu sendiri dapat mempengaruhi perangkat keras komputer, maka perlu untuk menggunakan sistem deteksi yang sensitif terhadap asap dan produk pembakaran lainnya.
- Detektor asap dan api harus ditransfer ke panel alarm pusat yang terus dipantau setiap saat dan dikirimkan berulang secara instan ke rumah pemadam kebakaran terdekat. Jika koneksi permanen ke rumah pemadam kebakaran tidak memungkinkan, setidaknya ada alarm eksternal untuk memberitahu orang di luar gedung dan menaikkan alarm dengan layanan darurat.

3. Fire Prevention and Detection

Firefighting

- Di pusat data, banyak kerusakan dapat dilakukan oleh peralatan pemadam kebakaran sebagaimana halnya oleh api itu sendiri. Meskipun demikian, sistem pencegah kebakaran yang efektif harus tetap dipasang di pusat data.
- Pemadaman dengan unsur kimia yang paling sering digunakan adalah Halon 1301, namun kemudian ditinggalkan dan digantikan dengan FM200 yang lebih ramah lingkungan.
- Karbon dioksida juga dapat digunakan namun harus diperhatikan masalah keamanan ketika gas tersebut dilepaskan
- Sistem gas bersifat “one-shoot”, jika api tidak padam dengan sekali pemadaman, maka tidak ada kesempatan kedua, karena gas perlu diisi ulang atau dihubungkan ke sumber yang baru
- Pemadaman dengan gas lebih sesuai untuk perangkat komputasi

3. Fire Prevention and Detection

Firefighting

- Sistem pemadam dengan penyiram air terdapat dua jenis. Jenis pipa basah yang selalu terisi air dan dapat bereaksi segera. Jenis pipa kering yang mulai mengisi air ketika terdeteksi gejala dan memiliki jeda
- Sistem pemadaman menggunakan air banyak disukai atau diamanatkan oleh pemilik bangunan atau perusahaan asuransi. Sistem air juga sangat dianjurkan di area atau tempat penyimpanan yang mengandung bahan yang mudah terbakar.
- Sistem ini dapat bekerja terus hingga api berhasil dikendalikan. Meskipun air dapat merusak perangkat keras namun lebih aman untuk melindungi bangunan.
- Keputusan tentang cara apa yang digunakan untuk menahan api dipengaruhi banyak faktor, termasuk tujuan dan kekritisan operasi pusat data.

4. Intrusion Detection Systems

- Dalam konteks keamanan fisik, sistem deteksi intrusi berarti alat yang digunakan untuk mendeteksi aktivitas pada batas-batas fasilitas yang dilindungi.
- Ketika perusahaan berkomitmen secara fisik melindungi bangunan tempat staf bekerja dan tempat peralatan pemrosesan informasi, harus dilakukan analisis risiko yang lengkap dan, jika perlu pertimbangkan untuk memasang sistem deteksi intrusi perimeter.

4. Intrusion Detection Systems

- Sistem deteksi intrusi paling sederhana adalah patroli penjaga. Penjaga yang berjalan di koridor dan perimeter fasilitas sangat efektif dalam mengidentifikasi upaya untuk masuk ke fasilitas dan membunyikan alarm atau mengakhiri upaya dengan menantang pengganggu. Tentu saja, kekurangannya adalah bahwa patroli tidak bisa berada di semua titik fasilitas pada saat yang sama.

- Hal lain yang paling sederhana adalah melalui pemantauan video. Kamera video ditempatkan di lokasi di fasilitas di mana semua titik dalam perimeter dapat dipantau secara bersamaan. Saat upaya intrusi terdeteksi, alarm dapat dibunyikan.

4. Intrusion Detection Systems

Tujuan

- Tugas pertama dalam menentukan persyaratan sistem deteksi intrusi adalah menentukan apa yang harus dilindungi serta tingkat dan sifat ancamannya. Untuk ancaman umum, misalnya pertanyaan: Bagaimana cara sesuatu dari luar masuk ke dalam? Apakah tempat parkir aman? Bagaimana prosedur pemuatan dokumen? Bagaimana kontrol akses gedung yang ada? Dsb.

- Pertanyaan lain yang harus diajukan dalam mendefinisikan tujuan sistem deteksi intrusi berhubungan dengan sejarah fasilitas. Misalnya, apakah ada insiden parkir khusus, insiden lapangan, atau insiden pelanggaran properti / fasilitas? Apakah ada kekhawatiran umum yang dapat mencakup pelanggaran, penyerangan, atau intimidasi? Kapan kejadian terakhir dan bagaimana kondisinya? Dsb.

- Jawaban pertanyaan-pertanyaan di atas dapat membantu menentukan apa tujuan sistem deteksi intrusi (dan apa yg harus dicapai). Selanjutnya adalah merencanakan sistem itu sendiri.

4. Intrusion Detection Systems

Perencanaan

- Perencanaan seharusnya dilakukan dengan tujuan untuk memberikan solusi yang membahas:
  - ✓ Pengawasan
  - ✓ Kontrol
  - ✓ Keamanan fisik
  - ✓ Pemeliharaan
  - ✓ Latihan
- Selama perencanaan, sifat dari fasilitas dan isi dari fasilitas itu harus dipertimbangkan. Misalnya, persyaratan sistem deteksi intrusi untuk kampus pusat data yang dibangun secara khusus, yang didirikan di lingkungannya sendiri dan dikelilingi oleh pagar perimeter, sangat berbeda dari persyaratan untuk pusat data yang bertempat di lantai gudang sebuah gedung multistore di pusat kota.

4. Intrusion Detection Systems

Elemen

- Perencanaan harus menghasilkan rancangan desain yang sesuai dengan tempatnya. Unsur-unsur deteksi intrusi yang diperlukan akan tergantung pada fasilitas.

- Misalnya, pusat data khusus mungkin memerlukan pagar perimeter, penerangan di pagar dan di ruang antara pagar dan dinding fasilitas, kamera video, dan perimeter sistem untuk bangunan itu sendiri. Di sisi lain, fasilitas yang terdapat dalam gedung serbaguna akan membutuhkan sistem deteksi intrusi pada pintu, jendela, lantai, dinding, dan langit-langit hanya pada bagian yang berisi pusat data.

4. Intrusion Detection Systems

- Elemen yang harus dipertimbangkan ketika memasang sistem deteksi intrusi meliputi:
  - ✓ CCTV
  - ✓ Penerangan
  - ✓ Sensor deteksi gerak
  - ✓ Sensor panas
  - ✓ Sistem alarm untuk jendela dan pintu
  - ✓ Sensor "pecahan kaca" (sensor derau yang dapat mendeteksi suara yang dibuat oleh pecahan kaca)
  - ✓ Sensor tekanan untuk lantai dan tangga

4. Intrusion Detection Systems

Prosedur

- Apa pun alat atau teknologi yang digunakan dalam sistem deteksi intrusi, sistem akan gagal memberikan keamanan kecuali jika prosedur yang memadai diterapkan, dan pelatihan tentang prosedur tersebut diberikan kepada staf yang berkepentingan.
- Staf setidaknya dilatih dua kali setahun tentang arti alarm sistem deteksi intrusi dan bagaimana meresponsnya.
- Staf yang bertanggung jawab untuk memantau sistem deteksi intrusi harus diajari untuk mengenali upaya intrusi dan bagaimana merespons sesuai dengan skala respons (kapan waktu yang tepat untuk merespons secara langsung, kapan harus merespons dengan bantuan dari petugas fasilitas, dan kapan penegakan hukum harus dipanggil untuk bantuan).

5. Sample Physical Security Policy

Policy

It is the responsibility of the Company management to provide a safe and secure workplace for all employees.

Standards

- The Company offices will be protected from unauthorized access.
- Areas within buildings, which house sensitive information or high-risk equipment, will be protected against unauthorized access, fire, water, and other hazards.
- Devices, which are critical to the operation of company business processes, will be identified in the Company Business Impact Analysis (BIA) process and will be protected against power failure.

Responsibilities

- Senior management and the officers of the Company are required to maintain accurate records and to employ internal controls designed to safeguard company assets and property against unauthorized use or disposition.
- The Company assets include but are not limited to physical property, intellectual property, patents, trade secrets, copyrights, and trademarks.
- Additionally, it is the responsibility of company line management to ensure that staff is aware of, and fully complies with the company's security guidelines, and all relevant laws and regulations.

Compliance

- Management is responsible for conducting periodic reviews and audits to assure compliance with all policies, procedures, practices, standards, and guidelines.
- Employees who fail to comply with the policies will be treated as being in violation of the Employee Standards of Conduct and will be subject to appropriate corrective action.

6. Sample Data Centre Infrastructure

- Anixter

  https://www.anixter.com/en_us/services-and-solutions/solutions/data-center

- Google

  https://www.google.com/about/datacenters/

6. Sample Data Centre Infrastructure

- Aruba Cloud

  https://www.arubacloud.com/infrastructures.aspx

- Iron Mountain Boston

  https://www.google.com/about/datacenters/

7. Summary

- Sifat keamanan secara fisik terhadap pusat data seharusnya merupakan cincin pertahanan terpusat - dimana persyaratan untuk masuknya semakin dekat ke pusat cincin semakin sulit.
- Alasannya jelas, jika kita mengambil sejumlah tindakan pencegahan untuk melindungi informasi yang diakses pada perangkat di seluruh organisasi, maka setidaknya kita harus memastikan bahwa tidak ada kerusakan atau gangguan yang terjadi pada perangkat keras tempat informasi disimpan dan diproses.
- Karena itu, prinsip konsistensi harus tetap diterapkan. Buat apa membangun kontrol akses fisik dengan biaya beberapa juta dolar jika potensi kerusakan yang dapat dilakukan pada pusat data kurang dari beberapa puluh juta dolar.

End of File