Kontrol Keamanan Fisik

Physical Security Controls dalam Audit EDP

Memahami jenis-jenis pengamanan fisik pada komputer dan risiko ancaman fisik yang harus ditanggulangi untuk melindungi sistem komputer organisasi.

Fondasi Lingkungan Kontrol SI

Kontrol keamanan fisik atas perangkat keras komputer membentuk fondasi lingkungan kontrol sistem informasi (SI) organisasi. Kerusakan unit pengolahan sentral (CPU) dan perangkat periferal dapat terjadi akibat berbagai bahaya alami dan manusia.

Komponen Dasar Sistem

Unit pemroses sentral, sistem operasi, dan program aplikasi sebagai fondasi sistem komputasi.

Sistem Manajemen Database

Komponen keempat dimana data berada dan dikelola secara terstruktur.

Keamanan Menyeluruh

Perlindungan fisik yang komprehensif untuk semua komponen sistem.

Bahaya Alam yang Mengancam

Bencana Geologis

- Gempa bumi di wilayah pantai
- Letusan gunung berapi seperti Mount Saint Helens (1980)
- Tanah longsor akibat hujan lebat

Bencana Meteorologis

- Badai di pantai tenggara
- Tornado di dataran tengah
- Banjir dari hujan lebat
- Badai salju dan dingin ekstrem
- Kebakaran hutan

Tidak ada bagian dunia yang kebal terhadap bahaya alam. Gunung berapi seperti Kilauea dan Mauna Loa di Hawaii tetap aktif, sementara Mount Pinatubo di Filipina meletus dahsyat pada 1991 setelah tertidur 6 abad.

Semua organisasi harus memiliki kontrol internal yang membantu mengurangi dampak bencana pada kelangsungan operasi.

Bahaya Manusia yang Merusak

Bahaya manusia dapat sama merusaknya dengan bencana alam. Pengeboman Oklahoma City (1995) dan serangan World Trade Center (1993, 2001) menunjukkan skala kerusakan yang dapat terjadi.

Pencurian Perangkat

Lebih dari 200.000 laptop dicuri pada 1995, meningkat 39% dari tahun sebelumnya. Laptop yang dicuri dapat dijual hingga 50% dari harga eceran di pasar gelap.

Kasus VISA International

Musim gugur 1996: komputer desktop dicuri dari pusat data VISA di San Mateo, California, berisi informasi 300.000+ rekening kartu kredit tidak terenkripsi. Biaya penggantian mencapai $6 juta.

Pembakaran dan Kerusakan

Kejahatan yang dapat mengakibatkan kerusakan signifikan pada sumber daya komputer organisasi.

Bahaya Tidak Terlihat

Tidak seperti bahaya fisik yang terlihat, beberapa ancaman dapat merusak tanpa jejak yang jelas:

- **Lonjakan listrik** dapat menggoreng sirkuit komputer dan peralatan sekitarnya
- **Gangguan elektromagnetik** dapat mengakibatkan data hilang, rusak, atau terganggu
- **Interferensi frekuensi** dapat mengganggu komunikasi sistem

Kontrol keamanan fisik dalam banyak organisasi sangat tidak memadai untuk menghadapi ancaman-ancaman ini.

Peran Auditor: Mengidentifikasi kelemahan kontrol keamanan fisik yang signifikan dan menyampaikan rekomendasi untuk manajemen.

Prinsip Dasar Penempatan Peralatan

Salah satu pencegahan paling jelas namun sering diabaikan adalah menempatkan peralatan komputer utama di lokasi yang aman dari banjir dan bencana.

Hindari Ruang Bawah Tanah

Basement rentan terhadap banjir yang dapat merusak peralatan secara total.

Lantai Pertama Berisiko

Masih dapat terkena dampak banjir parah, meskipun lebih baik dari basement.

Lantai Dua atau Lebih Tinggi

Lokasi optimal yang melindungi peralatan dari banjir dan akses tidak sah.

Meskipun layanan mungkin terganggu karena listrik dan telekomunikasi, peralatan tidak memerlukan perbaikan atau penggantian mahal.

Jenis-Jenis Kontrol Keamanan Fisik

Kunci Fisik

Konvensional, elektronik, cipher, kombinasi, dan biometrik untuk mengontrol akses.

Penjaga Keamanan

Penghalang untuk pencurian dan aktivitas tidak sah, memantau kontrol kamera.

Kamera Pengintai

Video surveillance untuk pemantauan dan bukti kejadian keamanan.

Sistem Deteksi Darurat

Alarm kebakaran, asap, dan prosedur tanggap darurat.

Sistem HVAC

Pemanas, ventilasi, dan pendingin untuk lingkungan optimal komputer.

Asuransi

Perlindungan hardware, software, dan biaya pemulihan data.

Kontrol Keamanan Fisik Lanjutan

Prosedur Backup Berkala

Backup sistem, aplikasi, dan data secara teratur dengan rotasi media ke lokasi luar yang aman.

Daya Listrik Darurat

Sistem UPS (Uninterruptible Power Supply) dan generator untuk kontinuitas operasi.

Program Pemulihan Bisnis

BRP (Business Recovery Program) yang komprehensif, terkini, dan teruji secara berkala.

Administrator Cadangan

Administrator keamanan sistem cadangan yang terlatih untuk kontinuitas pengelolaan.

Kunci Konvensional: Garis Pertahanan

Kunci konvensional tetap menjadi salah satu kontrol paling efektif untuk mengendalikan akses ke ruang terlarang seperti ruang komputer utama, lemari kabel, dan ruang server.

Pengelolaan Kunci yang Efektif

- Petugas keamanan bertanggung jawab penuh
- Kontrak dengan penjual untuk instalasi dan penggantian
- Inventaris lengkap semua kunci dan pemegangnya
- Penyimpanan kunci cadangan yang aman

Jenis-Jenis Kunci

- **Kunci biasa:** Unik untuk setiap pintu
- **Kunci master:** Membuka semua pintu di area tertentu
- **Kunci grand master:** Membuka semua kunci di semua fasilitas

Inventaris kunci master dan grand master harus dijaga ketat dengan pemegang yang sangat dipercaya.

Studi Kasus: Penghentian Pemegang Kunci

Penanggung jawab keamanan fisik sebuah organisasi mengundurkan diri secara tiba-tiba dalam keadaan sulit. Ia memiliki kunci grand master untuk semua fasilitas organisasi.

1

Risiko Identifikasi

Kemungkinan duplikat kunci grand master telah dibuat sebelum pengembalian.

2

Analisis Biaya

Mengunci ulang semua pintu mahal dan menyebabkan ketidaknyamanan signifikan.

3

Keputusan Manajemen

Mengunci ulang semua fasilitas untuk memastikan keamanan penuh.

Pelajaran: Jaga jumlah pemegang kunci master dan grand master seminimal mungkin. Pertimbangkan pertahanan ganda dengan brankas yang memerlukan dua kunci terpisah untuk membuka.

Sistem Lencana Akses Elektronik

Sistem lencana akses elektronik memberikan keuntungan signifikan dibanding kunci konvensional dalam pengelolaan akses dan pemantauan aktivitas.

Fleksibilitas Pengelolaan

Lencana dapat dinonaktifkan tanpa perlu mengunci ulang pintu saat karyawan berhenti atau pindah.

Kontrol Waktu

Akses dapat dibatasi untuk waktu tertentu dan dipantau di luar jam kerja normal.

Jejak Audit

Semua aktivitas akses tercatat secara elektronik untuk pemantauan dan investigasi.

Cara Kerja Sistem

Pemegang lencana menempatkannya pada pembaca yang membaca informasi otorisasi dari chip komputer. Data dikirim ke program aplikasi di server pusat. Jika terotorisasi, perintah dikirim untuk membuka kunci.

Kelemahan Sistem Lencana Elektronik

Risiko Keamanan

1. **Kunci manual:** Pintu masih memiliki kunci konvensional yang dapat membuka tanpa jejak audit
2. **Peminjaman lencana:** Orang dapat meminjamkan kartu ke orang lain
3. **Kesalahan pemrograman:** Administrator dapat memberikan akses tidak terotorisasi
4. **Bug aplikasi:** Pemrograman salah dapat memungkinkan akses tidak sah

Penting untuk Auditor: Periksa inventaris kunci konvensional yang terkait dengan sistem lencana elektronik untuk memastikan keamanan menyeluruh.

Studi kasus menunjukkan aplikasi dengan database terpisah untuk nomor lencana dan nama pemegang, memungkinkan lencana aktif tanpa nama yang sesuai.

Studi Kasus: Sistem Lencana dengan Dua Bagian

Audit menemukan aplikasi lencana akses elektronik berbasis DOS dengan kelemahan desain serius di pusat data organisasi besar.

01

Penemuan Masalah

Lencana manajer berfungsi tetapi tidak muncul dalam daftar resmi pemegang lencana.

02

Investigasi Sistem

Database nomor lencana dan database nama pemegang terpisah tanpa referensi silang otomatis.

03

Identifikasi Risiko

Lencana aktif dapat ada tanpa nama, dan tidak ada cara otomatis untuk mendeteksinya.

04

Kelemahan Tambahan

MCU dengan tombol alih manual dapat mengunci semua pintu, file sandi tidak terenkripsi.

Rekomendasi Perbaikan Sistem Lencana

1. ### Antarmuka GUI Baru

   Desain aplikasi dengan GUI yang ramah pengguna, menghilangkan MCU dengan tombol alih manual.

2. ### Database Terpadu

   Satu database kontrol akses berisi nomor lencana, nama pemegang, dan kemampuan akses.

3. ### Laporan Rekonsiliasi

   Program laporan otomatis untuk mengidentifikasi nomor lencana aktif tanpa entri nama.

4. ### Enkripsi Sandi

   File sandi terenkripsi dengan algoritma aman, tidak dapat dilihat dari aplikasi atau sistem operasi.

5. ### Fitur Keamanan Sandi

   Implementasi panjang minimum sandi dan fitur kadaluarsa sandi otomatis.

Kelemahan Administrasi Keamanan

Audit database mengungkapkan beberapa kelemahan prosedur administrasi internal yang memerlukan perbaikan segera.

1

Lencana Karyawan Lama

Empat mantan karyawan masih memiliki lencana aktif. Tujuh karyawan memiliki lencana tambahan yang tidak diperlukan. Enam nama salah dimasukkan dalam aplikasi.

2

Pegawai Lembaga Sementara

Diberikan lencana tetapi tidak mengembalikannya setiap hari. Tidak tunduk pada pemeriksaan latar belakang yang sama dengan karyawan tetap.

3

Retensi Catatan Pendek

Catatan elektronik upaya akses hanya disimpan 90 hari sebelum ditimpa. Harus diarsipkan minimal satu tahun.

Jenis Kunci Fisik Lainnya

Kunci Cipher

Dibuka dengan memasukkan kode rahasia pada tombol di sebelah pintu. Masalah: kode harus diubah dan dikomunikasikan setiap kali ada perpindahan atau penghentian karyawan.

Kunci Kombinasi

Memerlukan serangkaian kombinasi angka pada dial. Digunakan untuk mengamankan sandi dan informasi kritis. Pertahanan ganda dengan dua orang mengetahui bagian kombinasi berbeda.

Kunci Biometrik

Mengotentikasi melalui fitur fisik unik: sidik jari, telapak tangan, iris mata, retina, wajah, atau suara. Mahal tetapi sangat aman untuk fasilitas sensitif.

Setelah serangan 11 September 2001, minat dalam sistem identifikasi biometrik meningkat signifikan. Kongres AS mempertimbangkan data biometrik pada chip terenkripsi di SIM.

Perkembangan Teknologi Biometrik

Biaya sistem biometrik menurun, memungkinkan aplikasi komersial lebih luas. Proyeksi menunjukkan pertumbuhan pasar yang signifikan.

$58M	$594M	65%
Penjualan 1999	Proyeksi 2003	Pangsa AS
Nilai pasar biometrik global pada tahun 1999	Perkiraan penjualan biometrik tahun 2003	Persentase pasar yang dibentuk oleh Amerika Serikat

Contoh Implementasi

- San Antonio City Employees Federal Credit Union: verifikasi telapak tangan untuk akses brankas
- Naval Weapons Credit Union: pembaca sidik jari di jendela kasir ($100.000 investasi)

Keterbatasan Sistem Biometrik

Peneliti Jepang Tsumtomu Matsumoto menunjukkan kelemahan sistem pengenalan sidik jari dengan menciptakan gambar palsu menggunakan gelatin (bahan Gummi Bears).

Metode yang digunakan:

1. Membuat cetakan dari sidik jari sukarelawan dengan gelatin
2. Mencabut sidik jari dari permukaan, meningkatkan secara digital, mencetak pada transparan

Hasil: Menipu 11 detektor berbeda dengan tingkat keberhasilan 70-90%.

Perbandingan Keamanan

- **Sidik jari:** 25-40 titik ukuran
- **Iris mata:** 250-266 titik ukuran

Iris mata adalah fitur paling kaya dan stabil, dibentuk oleh proses jaringan air mata alami yang menciptakan struktur unik di setiap mata.

Biaya dan persepsi invasi membuat identifikasi iris mata kurang praktis untuk aplikasi komersial, tetapi ideal untuk aplikasi militer dan sangat sensitif.

Piggybacking: Ancaman Universal

Piggybacking adalah metode dimana orang berwenang membuka pintu dan memungkinkan orang lain mengikuti tanpa menggunakan metode akses pribadi mereka.

Kesopanan Berbahaya

Dilakukan untuk kenyamanan dan kesopanan, tetapi dapat menyebabkan akses tidak sah.

Risiko di Perusahaan Besar

Tidak semua karyawan saling mengenal, sulit mendeteksi karyawan yang telah dihentikan.

Jejak Audit Hilang

Mengalahkan jejak audit dari sistem lencana elektronik dan biometrik.

Metode Pencegahan

- Penegakan ketat akses file tunggal oleh penjaga keamanan
- Pintu putar baja lantai ke langit-langit
- Kamera pengintai di pintu masuk dengan peninjauan tepat waktu
- "Deadman" atau perangkap dengan pintu di kedua ujung

Penjaga Keamanan: Komponen Penting

Penjaga keamanan merupakan penghalang untuk pencurian, bahaya di tempat kerja, dan kegiatan ilegal. Mereka membantu mengurangi piggybacking dan memantau kamera video.

Tanggung Jawab Utama

Pemeriksaan catatan kepolisian, pelatihan berkelanjutan, keterampilan observasi dan menulis yang sangat baik.

Persyaratan Kontrak

Jangka waktu, biaya, pelatihan, kinerja, kewajiban, ganti rugi, dan persyaratan penghentian.

Sertifikasi Keselamatan

Pertolongan pertama dan CPR untuk situasi darurat di fasilitas.

Laporan insiden yang mereka persiapkan dapat menjadi bukti penting dalam kasus kriminal dan kesalahan karyawan. Keterampilan menulis yang baik sangat krusial untuk kredibilitas laporan.

Sistem Keamanan Tambahan

Kamera Pengintai Video

Kontrol tambahan yang bertindak sebagai penghalang efektif dan memberikan bukti kritis. Sistem harus menampilkan hari, tanggal, dan waktu pada rekaman. Monitor dipasang di pos penjaga dengan rotasi tampilan berkala.

Alarm dan Deteksi Darurat

Alarm dipicu oleh asap, api, atau tindakan tertentu. Dipantau elektronik terus-menerus oleh penjaga keamanan dan pemadam kebakaran lokal. Sistem penyiraman air aktif diperlukan di sebagian besar fasilitas.

Sistem HVAC

Komputer bertahan terbaik dalam lingkungan dingin, kering, dan bebas debu. Mainframe besar memerlukan AC khusus dan peralatan penghilang debu. Pemeliharaan rutin sangat penting untuk kesehatan staf.

Asuransi dan Backup: Perlindungan Ganda

Pertanggungan Asuransi

Asuransi harus melindungi:

- Perangkat keras pada biaya penggantian
- Perangkat lunak pada biaya penggantian
- Biaya untuk mengembalikan data yang hilang
- Kehilangan pendapatan (opsional, mahal)

Polis menetapkan prosedur tertentu: backup harian/mingguan/bulanan, penyimpanan di lokasi luar aman, pemeliharaan rutin sesuai spesifikasi pabrik.

Prosedur Backup Berkala

Backup harus dilakukan:

- **Harian:** Data yang berubah setiap hari
- **Mingguan/Bulanan:** Sistem penuh termasuk perangkat lunak
- **Setelah upgrade:** Perubahan signifikan sistem

Media cadangan harus dipindahkan ke lokasi luar yang aman dengan catatan terdokumentasi. Auditor harus mengunjungi fasilitas penyimpanan untuk mengevaluasi kontrol keamanan fisiknya.

Daya Listrik Darurat dan UPS

Sistem daya listrik darurat dan UPS (Uninterruptible Power Supply) harus dirancang ke dalam setiap fasilitas pengolahan informasi untuk memastikan kontinuitas operasi.

Generator Darurat

Generator diesel mampu menghasilkan 350+ kilowatt. Aktif otomatis dalam 10 detik saat kehilangan daya. Tangki 650 galon untuk operasi 24 jam.

Sistem UPS

Susunan baterai 100+ kilowatt. Memberikan listrik terus-menerus, meminimalkan lonjakan. Bertindak sebagai penyangga hingga generator aktif penuh.

Kontinuitas Terjamin

UPS dapat memberikan daya hingga 45 menit jika generator gagal. Kontrak pemeliharaan triwulanan dan semesteran dengan penjual.

Program Pemulihan Bisnis (BRP)

Setiap organisasi harus memiliki BRP yang terkini dan teruji. Program ini tidak harus berukuran ensiklopedia, tetapi singkat, ringkas, dan mudah dibaca sambil mempertahankan prosedur utama.

01

Daftar Kontak

Anggota utama dengan nomor telepon (rumah, kantor, ponsel, pager) dan alamat rumah.

02

Situs Kantor Alternatif

Lokasi utama dan kedua dimana manajemen dapat bersidang jika lokasi utama tidak dapat dioperasi.

03

Area Operasional Kritis

Identifikasi dan penggolongan area berisiko tinggi yang harus dipulihkan pertama kali.

04

Prosedur Pemicu

Kejadian yang memicu BRP, prosedur awal, dan prosedur peningkatan berdasarkan tingkat keparahan.

05

Tindakan per Area

Deskripsi ringkas tindakan di setiap area operasional dengan gambar dan skema fasilitas.

06

Dukungan Psikologis

Dampak psikologis bencana pada karyawan, prioritas keselamatan keluarga, konseling trauma.

Situs Pemulihan dan Administrator Cadangan

Jenis Situs Pemulihan

Situs Panas: Fasilitas penuh, operasional <24 jam. Mahal tetapi cepat.

Situs Dingin: Infrastruktur dasar tanpa peralatan. Murah tetapi lambat (beberapa minggu).

Situs Penjual: Fasilitas dari penjual khusus. Cepat tetapi biaya tinggi dan risiko ketidakcocokan.

Situs Timbal Balik: Perjanjian dengan organisasi lain. Murah tetapi risiko ketidakcocokan platform dan penegakan.

Administrator Sistem Cadangan

Sangat penting untuk kontinuitas operasi. Banyak organisasi gagal mengenali keperluan ini.

Risiko tanpa administrator cadangan:

- Satu orang dapat melakukan aktivitas tidak sah
- Sistem tidak dapat dipulihkan jika administrator tidak tersedia
- Kecelakaan atau penghentian tiba-tiba melumpuhkan operasi

Pilih administrator cadangan dengan hati-hati untuk menjaga pemisahan tugas yang memadai.