Keamanan Sistem Informasi - Pertemuan 2

HENDRI PURNOMO

Tujuan Pembelajaran

- Menjelaskan konsep dasar ancaman dan kerentanan dalam sistem informasi.
- Memahami mekanisme kontrol keamanan informasi.
- Mengetahui prinsip-prinsip dasar dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad).

CIA Triad

- Kerahasiaan (Confidentiality):
- Melindungi informasi dari akses yang tidak sah.
- Integritas (Integrity):
- Memastikan bahwa informasi tetap akurat dan tidak berubah oleh pihak yang tidak berwenang.
- Ketersediaan (Availability):
- Memastikan bahwa informasi dapat diakses oleh pihak yang berwenang saat dibutuhkan

Ancaman terhadap Sistem Informasi

- Definisi Ancaman: Potensi kejadian yang dapat merusak atau menghancurkan sistem informasi.
- Jenis Ancaman:
- - Serangan siber (malware, phishing, hacking)
- - Bencana alam (banjir, kebakaran)
- - Kesalahan manusia (human error)

Kerentanan (Vulnerability)

- Definisi Kerentanan: Kelemahan dalam sistem informasi yang dapat dieksploitasi oleh ancaman.
- Contoh:
- - Sistem yang tidak di-update (patch management)
- - Konfigurasi keamanan yang lemah

Mekanisme Kontrol Keamanan Informasi

- Kontrol Preventif: Mencegah terjadinya ancaman, seperti firewall dan enkripsi.
- Kontrol Detektif: Mendeteksi ketika ancaman terjadi, seperti IDS/IPS.
- Kontrol Korektif: Mengambil langkah perbaikan setelah ancaman terjadi, seperti backup dan recovery.

Jenis-jenis Serangan Siber

- Malware: Virus, worm, trojan, ransomware
- Phishing: Teknik social engineering untuk mendapatkan data sensitif
- DoS/DDoS (Denial of Service): Membanjiri sistem dengan permintaan agar layanan tidak tersedia

Protokol dan Standar Keamanan

- SSL/TLS: Protokol untuk mengamankan komunikasi melalui internet.
- ISO/IEC 27001: Standar manajemen keamanan informasi.
- NIST Cybersecurity Framework: Panduan untuk mengelola dan mengurangi risiko keamanan informasi.

Studi Kasus Keamanan Sistem Informasi

- Studi Kasus: Serangan WannaCry (Ransomware)
- Deskripsi serangan
- Dampak global
- Pelajaran yang bisa diambil

Praktik Terbaik Keamanan Sistem Informasi

- Memperbarui sistem dan aplikasi secara berkala.
- Menggunakan autentikasi dua faktor.
- Pelatihan keamanan untuk semua pengguna.
- Backup data secara berkala.

Diskusi dan Tugas

- Diskusikan mengenai insiden keamanan informasi yang pernah terjadi di lingkungan sekitar.
- Tugas: Identifikasi kerentanan dan ancaman pada sistem informasi yang sering digunakan sehari-hari.