UTS KEAMANAN INFORMASI

NAMA : MUHAMAD SATRIO ABEL FIKRI

NIM : 20230801100

Dosen : 7800 – Hani Dewi Ariessanti

Matkul : CIE406 – Keamanan Informasi KJ002

---

1. Jelaskan menurut Anda apa itu keamanan informasi!

Keamanan informasi adalah serangkaian langkah dan proses yang dilakukan untuk melindungi data atau informasi dari akses yang tidak sah, perubahan yang tidak diinginkan, pencurian, ataupun perusakan. Tujuannya adalah untuk memastikan bahwa informasi hanya bisa diakses oleh orang yang berwenang, tidak diubah tanpa izin, dan selalu tersedia saat dibutuhkan. Keamanan informasi mencakup aspek teknis (seperti firewall dan antivirus), prosedural (seperti kebijakan akses), serta edukasi pengguna.

2. Jelaskan menurut Anda apa itu Confidentiality, Integrity, dan Availability!

Ketiga istilah ini dikenal sebagai prinsip dasar dari keamanan informasi atau sering disebut sebagai CIA Triad:

- Confidentiality (Kerahasiaan):
  Merupakan upaya untuk menjaga agar informasi tidak bocor atau diakses oleh pihak yang tidak memiliki hak. Contohnya adalah penggunaan password, enkripsi, dan kontrol akses yang membatasi siapa saja yang bisa melihat informasi tersebut.
- Integrity (Integritas):
  Mengacu pada keaslian dan keakuratan data, yakni memastikan bahwa informasi tidak diubah tanpa izin selama proses penyimpanan, pemrosesan, atau pengiriman. Misalnya, penggunaan sistem checksum atau hash untuk mendeteksi perubahan data.
- Availability (Ketersediaan):
  Menjamin bahwa sistem dan data selalu bisa diakses oleh pengguna yang berwenang kapan saja mereka membutuhkannya. Contoh penerapannya adalah backup data, pemeliharaan server, dan sistem redundansi agar tetap berjalan meskipun terjadi gangguan.

3. Sebutkan jenis-jenis kerentanan keamanan yang Anda ketahui!

Kerentanan keamanan (security vulnerabilities) adalah celah atau kelemahan dalam sistem yang bisa dimanfaatkan oleh peretas atau pihak tak bertanggung jawab. Beberapa contohnya:

- Phishing: Penipuan yang dilakukan dengan cara menyamar sebagai pihak terpercaya untuk mencuri informasi penting seperti password dan data kartu kredit.
- Malware (Malicious Software): Program jahat seperti virus, worm, atau ransomware yang bisa merusak atau mencuri data.
- SQL Injection: Teknik serangan dengan menyisipkan kode SQL berbahaya ke dalam input data untuk mengakses atau mengubah data di dalam database.
- Man-in-the-Middle (MitM): Serangan di mana pelaku menyadap komunikasi antara dua pihak untuk mencuri data atau memanipulasi pesan.
- Brute Force Attack: Serangan dengan mencoba berbagai kombinasi password secara otomatis hingga menemukan yang benar.

4. Pengamanan data bisa menggunakan hash dan encryption. Jelaskan apa yang Anda ketahui terkait hash dan encryption!

- Hash:
  Hash adalah proses mengubah data menjadi kode unik tetap panjang, yang disebut hash value. Fungsi hash bersifat satu arah dan tidak bisa dikembalikan ke bentuk aslinya. Hash digunakan untuk memverifikasi integritas data, misalnya untuk memastikan file yang diunduh tidak diubah.
- Encryption (Enkripsi):
  Enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak bisa dibaca (ciphertext), kecuali dengan kunci tertentu. Tujuan enkripsi adalah menjaga kerahasiaan data saat dikirim atau disimpan.

5. Jelaskan menurut Anda apa itu session dan authentication!

- Session:
  Session adalah periode interaksi antara pengguna dengan sistem komputer atau aplikasi setelah login dan sebelum logout. Selama session berlangsung, sistem menyimpan data pengguna sementara (seperti identitas atau preferensi) untuk memudahkan proses dan menjaga pengalaman pengguna. Misalnya, saat kita login ke akun email, session akan memastikan bahwa kita tetap masuk tanpa perlu login ulang setiap klik.
- Authentication (Otentikasi):
  Authentication adalah proses untuk memverifikasi bahwa seseorang benar-benar adalah siapa yang mereka klaim. Proses ini biasanya dilakukan dengan memasukkan username dan password. Bentuk otentikasi lain bisa berupa OTP (One-Time Password), biometrik (sidik jari, wajah), atau token digital.

6. Jelaskan menurut Anda apa itu privacy dan ISO!

- Privacy (Privasi):
  Privasi adalah hak individu untuk mengontrol informasi pribadinya, termasuk bagaimana informasi itu dikumpulkan, digunakan, disimpan, dan dibagikan. Dalam konteks digital, menjaga privasi berarti melindungi data seperti alamat, nomor telepon, riwayat pencarian, dan kebiasaan pengguna dari penyalahgunaan.
- ISO (International Organization for Standardization):
  ISO adalah lembaga internasional yang menetapkan berbagai standar global, termasuk standar untuk keamanan informasi. Salah satu standar yang relevan adalah ISO/IEC 27001, yang memberikan kerangka kerja untuk membangun, mengelola, dan meningkatkan sistem manajemen keamanan informasi (ISMS). Sertifikasi ISO menunjukkan bahwa suatu organisasi serius dalam menjaga keamanan data.