UTS Keamanan Infiormasi

Nama: Arya Wicaksana

NIM: 20230801046

Dosen: HANI DEWI ARIESSANTI , S.Kom, M.Kom

KJ002

---

1. Pengertian Keamanan Informasi

Keamanan informasi adalah upaya untuk melindungi data dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Tujuan utamanya adalah memastikan kerahasiaan , integritas , dan ketersediaan informasi.

2. Tiga Pilar Utama Keamanan Informasi (CIA Triad)

- Confidentiality (Kerahasiaan): Memastikan hanya pihak yang berwenang yang dapat mengakses informasi.
- Integrity (Integritas): Memastikan bahwa data tidak diubah atau dirusak tanpa izin.
- Availability (Ketersediaan): Memastikan bahwa informasi tersedia bagi pengguna yang berwenang saat dibutuhkan.

3. Jenis-Jenis Kerentanan Keamanan yang Umum

- Peretasan (Hacking): Akses tidak sah ke sistem atau data.
- Malware (Perangkat Lunak Jahat): Program yang dirancang untuk merusak atau mengganggu sistem.
- Serangan Denial of Service (DoS): Upaya untuk memblokir akses ke sistem atau layanan.
- Social Engineering: Manipulasi psikologis terhadap pengguna untuk memperoleh informasi sensitif.
- Phishing: Penipuan online untuk mencuri informasi pribadi.
- Bug Perangkat Lunak: Kesalahan dalam kode program yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab.
- Kekurangan Konfigurasi: Sistem yang tidak dikonfigurasi dengan benar sehingga membuka celah keamanan.

4. Perbedaan Hash dan Enkripsi

- Hash:

Proses mengubah data menjadi nilai unik tetap (hash value). Hash bersifat satu arah (tidak dapat dibalik) dan digunakan untuk memastikan integritas data.

- Enkripsi (Encryption):

Proses mengubah data menjadi bentuk tidak terbaca (ciphertext) yang hanya bisa dikembalikan ke bentuk aslinya dengan kunci dekripsi. Digunakan untuk menjaga kerahasiaan data.

5. Authentication dan Session dalam Keamanan Sistem

- Authentication:

Proses verifikasi identitas pengguna. Contoh: login menggunakan username dan password.

- Session:

Periode aktif di mana pengguna dapat mengakses sistem setelah berhasil autentikasi. Digunakan untuk melacak dan membatasi akses pengguna.

6. Perbedaan Privacy dan ISO

- Privacy:

Hak individu atas informasi pribadinya, termasuk bagaimana data dikumpulkan, digunakan, dan disimpan.

- ISO (International Organization for Standardization):

Organisasi internasional yang menetapkan standar global, termasuk ISO 27001 yang mengatur sistem manajemen keamanan informasi.