UTS CIE406 - Keamanan Informasi

Nama : Defanda Yeremia

NIM : 20230801205

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

Hari/tgl : Selasa, 20 Mei 2025

Waktu : 15.30 - 17.30

Take Home Test

1. Jelaskan menurut anda apa itu keamanan informasi!

Menurut saya, keamanan informasi adalah upaya untuk menjaga data atau informasi agar tetap aman dari akses yang tidak sah, gangguan, ataupun kerusakan. Ini mencakup perlindungan terhadap informasi yang bersifat penting, rahasia, atau pribadi agar tidak bocor, dimanipulasi, atau hilang. Dalam dunia digital saat ini, keamanan informasi sangat penting karena hampir semua aktivitas manusia melibatkan data, baik itu data pribadi, data organisasi, maupun data keuangan. Tujuan utama dari keamanan informasi adalah memastikan bahwa informasi hanya bisa diakses oleh orang yang berhak, tetap akurat, dan tersedia ketika dibutuhkan.

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

Menurut saya, *Confidentiality* itu artinya menjaga agar informasi tetap rahasia dan hanya bisa diakses oleh orang yang berhak. Misalnya, data pribadi kita tidak boleh sembarang orang bisa lihat.
Lalu,
Integrity berarti menjaga agar informasi tidak berubah-ubah atau dirusak, jadi datanya tetap asli dan bisa dipercaya. Misalnya, kalau kita kirim file ke orang lain, isi file-nya tidak boleh berubah di tengah jalan.
Sedangkan
Availability artinya informasi atau sistem harus bisa diakses kapan saja saat

dibutuhkan, misalnya kalau kita mau akses data penting, sistemnya harus tetap bisa dibuka dan tidak error.

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

Beberapa jenis kerentanan keamanan yang saya ketahui antara lain adalah *phishing*, yaitu upaya untuk menipu pengguna agar memberikan informasi pribadi seperti password; *SQL injection*, di mana hacker menyisipkan perintah SQL berbahaya ke dalam sistem; serta *malware*, yang merupakan perangkat lunak berbahaya seperti virus atau ransomware yang dapat merusak sistem atau mencuri data.

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

Menurut pemahaman saya, *hash* dan *encryption* adalah dua teknik yang sering digunakan untuk melindungi data. *Hash* adalah proses mengubah data menjadi serangkaian karakter unik dengan panjang tetap. Fungsi hash bersifat satu arah, artinya data yang sudah di-*hash* tidak bisa dikembalikan ke bentuk aslinya. Biasanya hash digunakan untuk menyimpan password secara aman. Sedangkan *encryption* atau enkripsi adalah proses menyandikan data agar tidak bisa dibaca oleh pihak yang tidak berwenang. Berbeda dengan hash, enkripsi bersifat dua arah, artinya data bisa dikembalikan ke bentuk aslinya melalui proses dekripsi. Enkripsi digunakan dalam banyak hal seperti pengiriman pesan atau penyimpanan data penting agar tetap aman.

5. Jelaskan menurut anda apa itu session dan authentication!

Session menurut saya adalah waktu atau periode ketika pengguna sedang berinteraksi dengan suatu sistem. Misalnya saat kita login ke website, sistem akan membuat *session* untuk menyimpan status login kita sampai kita logout atau sesi habis. Session ini penting untuk menjaga pengalaman pengguna dan keamanan. Sementara itu, *authentication* adalah proses verifikasi identitas pengguna. Contohnya adalah saat kita login menggunakan username dan password. Tujuannya adalah untuk memastikan bahwa orang yang mengakses sistem benar-benar orang yang berhak. Kombinasi antara session dan authentication sangat penting agar sistem tetap aman dan nyaman digunakan.

6. Jelaskan menurut anda apa itu privacy dan ISO!

Menurut saya, *privacy* atau privasi adalah hak seseorang untuk menjaga data pribadinya agar tidak diakses atau digunakan oleh orang lain tanpa izin. Dalam dunia digital, privasi jadi sangat penting karena banyak data pribadi seperti nama, alamat, nomor KTP, atau bahkan kebiasaan pengguna bisa tersebar jika tidak dilindungi dengan baik. Privasi juga erat kaitannya dengan rasa aman, karena jika data kita bocor, bisa menimbulkan risiko seperti penipuan atau penyalahgunaan identitas.
Sedangkan
ISO, sejujurnya saya belum begitu paham secara mendalam, tapi yang saya tahu ISO adalah semacam organisasi internasional yang menetapkan standar-standar tertentu agar suatu sistem bisa diakui secara global. Dalam konteks keamanan informasi, saya pernah dengar tentang ISO 27001, yaitu standar yang digunakan untuk mengatur bagaimana perusahaan atau organisasi bisa mengelola keamanan data mereka. Walaupun saya belum mempelajari secara lengkap, saya mengerti bahwa sertifikasi ISO itu penting sebagai bukti bahwa suatu organisasi punya sistem keamanan informasi yang baik.