Nama: Edoardo Joseph Sila

NIM: 20230801143

1. Jelaskan menurut anda apa itu keamanan informasi!
   Jawaban:
   Keamanan informasi adalah serangkaian upaya dan proses yang dilakukan untuk melindungi data atau informasi, baik dalam bentuk digital maupun fisik, dari berbagai ancaman seperti akses ilegal, penyalahgunaan, perubahan, kerusakan, atau pencurian. Tujuan utama keamanan informasi adalah memastikan kerahasiaan, keutuhan, dan ketersediaan informasi tetap terjaga. Di era digital sekarang ini, keamanan informasi sangat penting karena hampir seluruh aktivitas bisnis, pemerintahan, dan individu sangat bergantung pada data yang harus dilindungi dari ancaman siber maupun ancaman dari dalam organisasi. Pelaksanaan keamanan informasi melibatkan kebijakan, prosedur, teknologi, serta peningkatan kesadaran dan edukasi kepada seluruh pihak terkait agar risiko dapat diminimalisir.

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

   Confidentiality, Integrity, dan Availability adalah tiga aspek utama dalam keamanan informasi yang sering disebut CIA Triad. Confidentiality berarti memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi, sehingga data tidak jatuh ke tangan yang tidak berhak. Integrity adalah menjaga agar informasi tetap akurat, konsisten, dan tidak berubah tanpa izin, baik secara sengaja maupun tidak sengaja. Availability menjamin bahwa informasi dan sistem selalu dapat diakses oleh pihak yang berhak saat diperlukan. Ketiga aspek ini saling terkait dan menjadi dasar dalam penerapan sistem keamanan informasi di berbagai organisasi.

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

   Jawaban:

   Ada banyak jenis kerentanan yang dapat ditemukan pada sistem informasi, di antaranya:

   - Kerentanan perangkat lunak, seperti bug, celah kode, dan konfigurasi aplikasi yang lemah.

- Kerentanan jaringan, seperti port terbuka yang tidak terlindungi, serangan man-in-the-middle, dan pencurian data melalui sniffing.
- Kerentanan perangkat keras, misalnya firmware yang tidak diperbarui.
- Kerentanan sosial, yang memanfaatkan kelemahan manusia, seperti phishing, pretexting, dan baiting.

Selain itu, kebijakan dan prosedur keamanan yang lemah, misalnya penggunaan kata sandi yang mudah ditebak, kurangnya pelatihan keamanan, atau tidak adanya backup data rutin juga merupakan sumber kerentanan.

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

   Jawaban:

   Hash dan enkripsi adalah dua teknik pengamanan data dengan fungsi berbeda. Hash adalah proses mengubah data menjadi rangkaian karakter unik menggunakan algoritma tertentu (misalnya SHA-256 atau MD5). Hash bersifat satu arah, sehingga data yang sudah di-hash tidak dapat dikembalikan ke bentuk aslinya. Hash biasa digunakan untuk memverifikasi data, seperti menyimpan kata sandi atau memeriksa integritas file. Enkripsi adalah proses mengubah data asli (plaintext) menjadi bentuk tidak terbaca (ciphertext) menggunakan algoritma dan kunci tertentu. Enkripsi bersifat dua arah, yang berarti data dapat dikembalikan ke bentuk aslinya lewat dekripsi jika memiliki kunci yang benar. Enkripsi digunakan untuk menjaga kerahasiaan data selama pengiriman atau penyimpanan agar hanya pihak berwenang yang bisa mengaksesnya.

5. Jelaskan menurut anda apa itu session dan authentication!

   Jawaban:

   Session adalah rentang waktu di mana pengguna berinteraksi dengan sistem setelah melakukan login, di mana sistem mengenali pengguna tersebut sampai sesi berakhir atau pengguna logout. Session biasanya menyimpan data sementara mengenai status login dan aktivitas pengguna agar tidak perlu melakukan otentikasi berulang saat mengakses halaman berbeda dalam aplikasi atau website. Authentication (otentikasi) adalah proses memverifikasi identitas pengguna sebelum memberikan akses ke sistem atau data, yang bisa menggunakan metode seperti password, PIN, biometrik, atau two-factor

authentication. Authentication penting agar hanya pengguna yang sah yang dapat mengakses layanan atau data tertentu.

6. Jelaskan menurut anda apa itu privacy dan ISO!

   Jawaban:

   Privacy (privasi) adalah hak individu atau organisasi untuk mengontrol informasi pribadi mereka serta membatasi siapa yang dapat mengakses, menggunakan, atau membagikan data tersebut. Dalam konteks teknologi, privasi berarti perlindungan data pribadi agar tidak disalahgunakan atau diakses tanpa izin dari pihak internal maupun eksternal. ISO (International Organization for Standardization) adalah organisasi internasional yang membuat standar global di berbagai bidang, termasuk keamanan informasi. Contohnya adalah ISO/IEC 27001, standar internasional untuk sistem manajemen keamanan informasi (Information Security Management System/ISMS) yang memberikan kerangka kerja dan panduan bagi organisasi dalam mengelola dan melindungi data secara sistematis dan berkelanjutan.