Nama : Damar Subekti

Nim : 20210801244

1. Jelaskan menurut anda apa itu keamanan informasi!
   Keamanan informasi adalah suatu disiplin ilmu dan praktik yang berfokus pada perlindungan informasi dan sistem informasi dari berbagai ancaman yang dapat merusak kerahasiaan, integritas, dan ketersediaannya (sering disebut sebagai Triad CIA). Dalam era digital saat ini, di mana data menjadi aset yang sangat berharga bagi individu maupun organisasi, menjaga keamanan informasi menjadi krusial. Keamanan informasi tidak hanya melibatkan aspek teknis, seperti penggunaan firewall atau enkripsi, tetapi juga aspek prosedural, kebijakan, dan kesadaran sumber daya manusia. Tujuannya adalah untuk meminimalkan risiko kerugian, kerusakan, atau penyalahgunaan informasi, serta memastikan keberlangsungan bisnis dan kepatuhan terhadap regulasi yang berlaku. Lebih dari sekadar pencegahan terhadap serangan siber, keamanan informasi juga mencakup penanganan insiden, pemulihan pasca-bencana, dan manajemen risiko secara berkelanjutan. Ini adalah pendekatan holistik yang terus berkembang seiring dengan munculnya ancaman dan teknologi baru.

2. Jelaskan menurut anda apa itu Confidentiality, Integrity and Availability!
   Konsep Confidentiality, Integrity, dan Availability (CIA Triad) merupakan fondasi utama dalam model keamanan informasi, yang digunakan untuk mengidentifikasi dan mengkategorikan tujuan-tujuan utama dalam melindungi informasi.
   a. Confidentiality (Kerahasiaan):
      Kerahasiaan adalah prinsip yang memastikan bahwa informasi hanya dapat diakses, diungkapkan, atau ditunjukkan kepada pihak yang berwenang (otorisasi) saja. Ini berarti informasi sensitif harus dijaga kerahasiaannya dan tidak boleh diungkapkan kepada individu, entitas, atau proses yang tidak sah.
   b. Integrity (Integritas):
      Integritas adalah prinsip yang menjamin bahwa informasi akurat, lengkap, konsisten, dan tidak mengalami perubahan atau modifikasi tanpa otorisasi. Ini berarti data harus tetap dalam kondisi aslinya dan tidak boleh dirusak atau diubah secara sengaja maupun tidak sengaja oleh pihak yang tidak berwenang. Tujuan integritas adalah untuk memastikan kepercayaan dan keandalan data. Availability (Ketersediaan):
      Ketersediaan adalah prinsip yang memastikan bahwa sistem, layanan, dan informasi dapat diakses dan digunakan oleh pihak yang berwenang (otorisasi) kapan pun mereka membutuhkannya. Ini melindungi dari gangguan layanan yang dapat disebabkan oleh kegagalan perangkat keras/lunak, serangan siber (seperti Serangan Penolakan Layanan Terdistribusi/DDoS), atau bencana alam.

3. Sebutkan jenis-jenis jaminan keamanan yang anda ketahui!
   Jaminan keamanan (Security Controls) adalah mekanisme atau proses yang dirancang untuk melindungi aset informasi. Umumnya, jaminan keamanan dapat diklasifikasikan ke dalam beberapa jenis utama:
   a. Jaminan Teknis (Technical Controls):
      Ini adalah kontrol yang diimplementasikan melalui perangkat keras atau perangkat lunak untuk melindungi sistem dan data. Mereka seringkali bersifat otomatis dan beroperasi pada tingkat teknologi.
   b. Firewall: Perangkat keamanan jaringan yang memantau dan menyaring lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang ditetapkan.

c. Sistem Deteksi/Pencegahan Intrusi (IDS/IPS): Mampu mendeteksi (IDS) atau bahkan mencegah (IPS) aktivitas mencurigakan atau serangan yang ditujukan ke jaringan atau sistem.
d. Antivirus dan Anti-Malware: Perangkat lunak yang dirancang untuk mendeteksi, mencegah, dan menghapus malware (virus, trojan, ransomware, dll.).
e. Sistem Enkripsi: Teknologi yang menggunakan algoritma kriptografi untuk melindungi kerahasiaan data baik saat disimpan (data at rest) maupun saat dalam transmisi (data in transit).
f. Autentikasi Multi-Faktor (MFA): Membutuhkan lebih dari satu metode verifikasi dari kategori kredensial independen untuk membuktikan identitas pengguna (misalnya, kata sandi + kode OTP).

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

   Hash dan Encryption adalah dua teknik kriptografi fundamental yang sering digunakan dalam pengamanan data, namun memiliki tujuan dan cara kerja yang berbeda:

   a. Hashing (Fungsi Hash Kriptografi)

      Hashing adalah proses satu arah yang mengubah string input (data apa pun, berapapun ukurannya) menjadi string karakter tetap berukuran tetap yang disebut hash value, digest, atau fingerprint. Fungsi hash yang baik dirancang sedemikian rupa sehingga perubahan sekecil apa pun pada data input akan menghasilkan hash value yang sangat berbeda, dan sangat sulit untuk merekonstruksi data asli dari hash value tersebut (one-way function). Selain itu, probabilitas dua input yang berbeda menghasilkan hash value yang sama (disebut "kolisi") harus sangat rendah.

      Tujuan Utama: Integritas Data dan Keamanan Kata Sandi.

      Cara Kerja: Data input dimasukkan ke dalam algoritma hash (misalnya SHA-256). Algoritma ini akan memproses data tersebut dan menghasilkan hash value yang unik untuk input tersebut.

   b. Encryption (Enkripsi)

      Definisi: Enkripsi adalah proses dua arah yang mengubah data asli yang dapat dibaca (plaintext) menjadi data yang tidak dapat dibaca (ciphertext) menggunakan algoritma enkripsi dan kunci kriptografi. Tujuan utamanya adalah untuk memastikan kerahasiaan data. Data terenkripsi hanya dapat diubah kembali menjadi plaintext jika kunci dekripsi yang benar digunakan.

      Tujuan Utama: Kerahasiaan Data.

      Cara Kerja: Data plaintext dan kunci enkripsi dimasukkan ke dalam algoritma enkripsi. Hasilnya adalah ciphertext. Proses dekripsi adalah kebalikannya, menggunakan ciphertext dan kunci dekripsi untuk mendapatkan kembali plaintext.

5. Jelaskan menurut anda apa itu session dan authentication!

   A. Authentication (Otentikasi):

      Otentikasi adalah proses krusial dalam keamanan informasi yang bertujuan untuk memverifikasi identitas seorang pengguna, sistem, atau entitas lain. Sebelum akses ke sumber daya atau sistem diberikan, otentikasi harus dilakukan untuk memastikan bahwa subjek yang mencoba mengakses adalah benar-benar siapa yang mereka klaim.

      Tujuan: Membangun kepercayaan pada identitas.

      Bagaimana Ia Bekerja: Otentikasi biasanya didasarkan pada satu atau lebih faktor: Sesuatu yang Anda Ketahui (Knowledge Factor): Paling umum adalah kata sandi (password), PIN, atau frasa sandi (passphrase).

Sesuatu yang Anda Miliki (Possession Factor): Contohnya adalah token keamanan fisik (hardware token), kartu pintar, atau kode OTP (One-Time Password) yang dikirimkan ke ponsel melalui SMS atau aplikasi otentikator.
Sesuatu yang Anda (Biometric Factor): Ciri biologis unik seperti sidik jari, pemindaian retina, pengenalan wajah, atau suara.
Contoh: Ketika Anda login ke Facebook, Anda memasukkan username dan password Anda. Sistem akan memverifikasi apakah kombinasi tersebut cocok dengan catatan di database. Jika cocok, Anda berhasil diotentikasi.

B. Session (Sesi):
Setelah seorang pengguna berhasil melewati proses otentikasi, server akan membuat sebuah "sesi" untuk pengguna tersebut. Sesi adalah periode waktu di mana server mempertahankan informasi tentang status interaksi pengguna dengan aplikasi, sehingga pengguna tidak perlu melakukan otentikasi berulang kali untuk setiap permintaan.
Tujuan: Menyediakan pengalaman pengguna yang mulus dan mempertahankan status login.
Bagaimana Ia Bekerja:
Ketika otentikasi berhasil, server membuat ID sesi yang unik. ID sesi ini kemudian dikirimkan kembali ke browser pengguna, biasanya dalam bentuk cookie. Untuk setiap permintaan HTTP berikutnya, browser akan mengirimkan cookie yang berisi ID sesi kembali ke server. Server akan menggunakan ID sesi ini untuk mencari data sesi yang terkait (misalnya, informasi login pengguna, preferensi, item di keranjang belanja) dan memverifikasi bahwa pengguna masih diotentikasi dan berwenang.
Manajemen Sesi: Sesi harus dikelola dengan aman. Ini termasuk:
Sesi Timeout: Mengatur batas waktu setelah itu sesi akan berakhir secara otomatis jika tidak ada aktivitas.
Regenerasi ID Sesi: Mengubah ID sesi setelah otentikasi berhasil atau perubahan hak akses penting untuk mencegah session fixation attacks.
Penyimpanan Sesi Aman: Menyimpan data sesi di server (misalnya di database, cache, atau file sistem) dan tidak menyimpan informasi sensitif di cookie klien.
Contoh: Setelah Anda login ke Gmail, Anda tidak perlu memasukkan username dan password setiap kali Anda membuka email atau mengklik tautan lain di Gmail. Ini karena sesi Anda aktif dan browser Anda mengirimkan ID sesi ke server Gmail, yang mengenali Anda sebagai pengguna yang sudah diotentikasi.

6. Jelaskan menurut anda apa itu privacy dan ISO!
   A. Privacy (Privasi)
   Privasi dalam konteks keamanan informasi merujuk pada hak individu untuk mengontrol informasi pribadi mereka. Ini adalah kemampuan seseorang untuk menentukan kapan, bagaimana, dan sejauh mana informasi tentang dirinya dikumpulkan, digunakan, disimpan, dan dibagikan kepada orang lain. Konsep privasi sangat erat kaitannya dengan perlindungan data pribadi dan seringkali diatur oleh undang-undang dan peraturan yang ketat.
   B. ISO (International Organization for Standardization)

ISO adalah sebuah organisasi non-pemerintah internasional yang mengembangkan dan menerbitkan standar internasional sukarela. Standar ini mencakup berbagai sektor industri dan teknologi, termasuk keamanan informasi. Tujuan utama ISO adalah untuk memfasilitasi perdagangan global dengan menyediakan standar umum yang meningkatkan kualitas, keamanan, efisiensi, dan kompatibilitas produk, layanan, dan sistem.