UTS (ULANGAN TENGAH SEMESTER)
KEAMANAN INFORMASI

Nama: Rajih Asyam Driagrian - 202030801099

KJ003

Dosen Pengampu:
Hani Dewi Ariessanti, S.Kom, M.Kom

Jakarta, 20 Mei 2025

ESSAY

Jawaban:

1. Keamanan Informasi adalah berasal dari kata keamanan dan informasi. Keamanan itu sendiri memiliki definisi sebagai kemampuan mempertahankan diri (*survival*) dalam menghadapi ancaman yang nyata dan informasi sendiri memiliki arti adalah data yang sudah diolah menjadi bentuk yang bernilai dan bermakna. **Keamanan Informasi** adalah sekumpulan metodologi, praktik, ataupun proses yang dirancang dan diterapkan untuk melindungi informasi atau data pribadi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah.

2. *Confidentiality, Integrity dan Availability* adalah tiga konsep:
    - Confidentiality:
      Memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
    - Integrity:
      Memastikan bahwa data tetap akurat, lengkap, dan tidak berubah secara tidak sah.
    - Availability:
      Memastikan bahwa data dan sistem dapat diakses oleh pihak berwenang ketika dibutuhkan.

3. Kerentanan keamanan dapat diklasifikasikan menjadi beberapa jenis utama: kerentanan perangkat lunak, kerentanan sistem operasi, kerentanan jaringan, dan kerentanan manusia.
    - Kerentanan perangkat lunak
      bug di aplikasi web, perangkat lunak klien, atau server.
    - Kerentanan Sistem Operasi
    - Kerentanan Jaringan
      konfigurasi firewall yang salah, protokol enkripsi yang lemah, atau router yang mudah diakses.
    - Kerentanan Manusia
      serangan phishing, kebocoran informasi sensitif.

4. Hash dan enkripsi adalah 2 teknik yang berbeda yang digunakan dalam pengamanan data.
    - Hashing adalah proses mengubah data menjadi nilai unik dengan panjang tetap, yang disebut hash. Hashing memiliki fungsi satu arah, artinya tidak mungkin untuk mendapatkan data asli kembali dari nilai hash, sering digunakan untuk menyimpan kata sandi, memverifikasi tanda tangan digital, dan melindungi integritas data.
    - Enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca menggunakan algoritma dan kunci. Enkripsi melindungi kerahasiaan data, memastikan bahwa hanya pihak yang berwenang yang dapat membaca data.

5. Session adalah periode waktu ketika pengguna aktif berinteraksi dengan sebuah sistem atau aplikasi, seperti website. Autentikasi adalah proses memverifikasi identitas pengguna yang ingin mengakses suatu sistem, biasanya dengan meminta kredensial seperti username dan password.
    - Session digunakan untuk menjaga keamanan dan mempermudah pengalaman pengguna dengan menghindari proses login berulang untuk setiap interaksi.
    - Autentikasi memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem atau aplikasi. Ini biasanya melibatkan verifikasi kredensial pengguna, seperti username dan password, untuk memastikan bahwa mereka adalah orang yang mereka katakan. Setelah pengguna berhasil diautentikasi, sesi akan dimulai dan pengguna dapat melanjutkan interaksi dengan sistem tanpa perlu login lagi.

6. Privasi adalah hak setiap individu untuk memiliki kendali atas informasi pribadi. Ini meliputi hak untuk menentukan siapa yang dapat mengakses, menggunakan, dan memproses data pribadi. Privasi penting karena melindungi individu dari potensi penyalahgunaan informasi pribadi.
   ISO (International Organization for Standardization)
   ISO adalah organisasi internasional yang mengembangkan dan menerbitkan standar untuk berbagai industri dan bidang. Standar ISO memberikan pedoman untuk memastikan kualitas, keselamatan, dan keamanan. Standar ISO, organisasi dapat meningkatkan kepercayaan dari pelanggan, mitra, dan pemangku kepentingan lainnya, juga dapat mengurangi risiko terkait dengan pelanggaran privasi data, seperti denda atau tuntutan hukum.