UJIAN TENGAH SEMESTER KEAMANAN INFORMASI

Nama: Jaffarob Firjih Yansyah
NIM: 20230801460

1. Jelaskan menurut Anda apa itu keamanan informasi . . .
   Keamanan informasi adalah tindakan yang dilakukan demi mencegah akses, penggunaan, modifikasi, gangguan, dan perusakan yang tidak diinginkan sehingga kerahasiaan, integritas, dan ketersediaan informasi tetap terjamin.

2. Jelaskan menurut Anda apa itu *Confidentiality*, *Integrity*, dan *Availability* . . .
   Confidentiality (kerahasiaan) adalah bahwa informasi tidak dapat diakses secara bebas oleh pihak tidak berwenang, yang selanjutnya menjamin informasi tetap memenuhi nilai *Integrity* (integritas): akurat dan tidak bisa dimodifikasi tanpa izin. Ini memastikan informasi tetap ada (*Available*) saat dibutuhkan oleh pihak berwenang.

3. Sebutkan jenis-jenis kerentanan keamanan yang Anda ketahui . . .
   Secara garis besar, kerentanan keamanan terbagi menjadi 6 jenis:
   - Pertama, kerentanan perangkat lunak, yang merupakan celah pada kode perangkat lunak yang bisa dieksploitasi oleh pihak tak bertanggungjawab. Kerentanan perangkat lunak juga mencakup kerentanan dalam sistem operasi, peramban web, aplikasi web, dan aplikasi seluler. Contoh dari kerentanan ini adalah *Buffer Overflow*, *SQL Injection*, dan *Cross-Site Scripting*.
   - Kedua, kerentanan jaringan. Berkaitan dengan masalah infrastruktur, termasuk masalah konfigurasi jaringan, kurangnya pemantauan, dan ketidakamanan enkripsi. Data yang mengalir melalui jaringan dapat diintersep dan diakses oleh penyerang.
   - Ketiga, kerentanan manusia. Kerentanan ini disebabkan oleh perilaku lalai (*human error*) yang berdampak pada keamanan data, seperti berbagi sandi dengan orang lain, mengakses tautan *phising*, atau meninggalkan perangkat tanpa pengawasan dan penjagaan yang memadai.
   - Keempat, kerentanan fisik. Kerentanan ini disebabkan oleh akses fisik tidak sah pada perangkat, termasuk pencurian perangkat, penjebolan pusat data, dan akses fisik ke server.
   - Kelima, kerentanan konfigurasi. Kerentanan ini terkait dengan pengaturan perangkat keras atau perangkat lunak yang tidak aman, seperti pengaturan hak akses yang kurang ketat, atau pengaturan sandi yang mudah ditebak atau masih dalam kondisi default.
   - Keenam, kerentanan *patch*. Berkaitan dengan gagalnya organisasi dalam memperbarui aplikasi dengan *patch* terbaru. Penyerang dapat memanfaatkan celah yang belum ditutup oleh *patch* untuk pengaksesan tidak sah.

4. Pengamanan data bisa dilakukan dengan *hash* dan *encryption*. Jelaskan apa yang Anda ketahui terkait *hash* dan *encryption* . . .
   Hash adalah teknik yang dilakukan untuk mengubah teks informasi menjadi *string* tersandi yang tidak dapat dipulihkan ke teks asalnya. *Hash* berguna dalam autentikasi data dan penjagaan integritas data. Di sisi lain, enkripsi mengubah teks informasi menjadi *string*

tersandi yang dapat dipulihkan ke bentuk teks asalnya dengan kunci dekripsi. Enkripsi digunakan dalam menjaga kerahasiaan dan ketersediaan data dalam waktu yang bersamaan.

5. Jelaskan menurut Anda apa itu *session* dan *authentication* . . .
   - *Session* adalah jarak waktu yang terhitung sejak pengguna berinteraksi layanan dan berakhir ketika pengguna keluar dari layanan atau setelah selang waktu yang telah ditentukan. Setiap *session* memiliki identitas unik berupa *session ID*. *Session* memastikan data pengguna, seperti preferensi dan riwayat, dapat disimpan sementara waktu dalam server tanpa harus meminta pengguna memasukkan data tersebut berulangkali. *Session* juga menjamin keamanan sistem dan efisiensi penggunaan sistem dengan memastikan pengguna hanya bisa mengakses ke informasi tertentu berdasarkan *session ID* mereka.
   - *Authentication* adalah prosedur yang digunakan untuk memverifikasi identitas pengguna demi mencegah akses tidak sah. Prosedur ini memastikan bahwa pengguna adalah benar-benar individu yang mereka klaim.

6. Jelaskan menurut Anda apa itu *privacy* dan ISO . . .
   Privacy adalah hak individu untuk menjaga kerahasiaan dan kebebasan data pribadi mereka dari gangguan, baik dalam kehidupan pribadi maupun penggunaan informasi pribadi. Ini termasuk hak untuk mengontrol bagaimana data pribadi mereka dikumpulkan, digunakan, dan dibagikan. ISO (*International Organization for Standardization*) adalah organisasi internasional yang mengembangkan dan mempublikasikan standarisasi dalam bidang industri dan manajemen. Standarisasi ini dibuat untuk memperbaiki kualitas, efisiensi, dan konsistensi dalam berbagai sektor.