Dosen : Hani Dewi Ariessanti , S.Kom, M.Kom
Mahasiswa : Jiwanta Nabhan Alauddin
NIM : 20230801384
Mata Kuliah : Keamanan Informasi – KJ003 – CIE406

Soal Essay

1. Jelaskan menurut anda apa itu keamanan informasi!, Solusi:

   Menurut saya, keamanan informasi itu merupakan segala upaya yang kita lakukan dalam melindungi data data atau informasi supaya informasinya terjaga utuh, tetap rahasia serta dapat digunakan oleh orang yang berhak mulai dari proses pembuatannya, penyimpanannya dan pemrosesan informasi tersebut dikelola hingga dikirim maupun dimusnahka, biasanya dalam keamanan informasi ini usaha usaha yang dilakukan yang saya ketahui diantaranya mulai dari kebijakan, prosedur, maupun teknologi yang digunakan harus diperhatikan dalam upaya mengamankan suatu informasi. Dalam keamanan informasi terdapat 3 aspek yang penting yakni Confidentiality, Integrity, Availability (CIA) sebagaimana penjelasan saya berikut ini:

   1.1. Confidentiality (kerahasiaan) yakni data hanya boleh diakses oleh orang yang berhak.

   Jadi Confidentiality ini merupakan Upaya menjaga kerahasiaan informasi agar hanya orang, sistem, atau proses yang berwenang yang dapat melihat atau memakainya. Dalam praktiknya, organisasi menerapkan berbagai mekanisme seperti enkripsi, kata sandi yang kuat, autentikasi multi-faktor, serta kebijakan “least privilege” supaya data sensitive misalnya saja rekam medis pasien atau nomor kartu kredit supaya tidak bocor ke pihak yang salah. Tujuannya untuk mencegah pihak yang tidak berwanang atau tak sah mengintip, menyalin, atau menyebarkan isi informasi.

   1.2. Integrity (Integritas) yakni data harus tetap akurat dan tidak boleh diubah tanpa izin.

   Jadi Integrity menekankan bahwa informasi harus tetap utuh dan akurat, tidak boleh diubah secara tidak sah, baik sengaja maupun karena kesalahan teknis. Untuk menjamin integritas, digunakan teknik seperti hash checksum, tanda tangan digital, kontrol versi, dan audit log, sehingga setiap perubahan bisa dideteksi atau dipulihkan ke keadaan asli. Bayangkan aja kalau isi saldo di rekening bank kita berubah wkwkwk:v jika satu bit saja berubah tanpa prosedur resmi, konsekuensinya bisa fatal maka itulah sebabnya aspek integritas sangat krusial.

   1.3. Availability (Ketersediaan) yakni data dan sistem harus selalu bisa diakses oleh pengguna yang berhak.

   Jadi Availability ini memastikan bahwa data dan layanan selalu siap diakses tepat saat dibutuhkan oleh pengguna yang berhak. Ini dicapai dengan infrastruktur yang andal begitu pula pada server cadangan, koneksi jaringan redundant, sistem pemulihan bencana, dan pemantauan 24 jam serta prosedur teknis seperti load-balancing, fail-over, dan patch rutin. Tanpa ketersediaan, meski data sudah aman dan akurat, manfaatnya hilang; misalnya,

layanan mobile banking yang mati ketika nasabah mau transfer akan langsung merugikan bisnis dan menurunkan kepercayaan pengguna.

Dalam menjaga keamanan informasi sendiri banyak hal yang perlu dilakukan untuk menjaga keamanan data maupun informasi supaya tidak bocor atau terjadinya fabrikasi yakni data palsu yang ditambahkan dalam sistem, selain itu kemanan informasi dilakukan untuk menjaga data supaya datanya tidak dimanipulasi atau datanya dirubah oleh pengguna yang tidak sah atau pengguna tanpa izin, beberapa diantaranya yang harus diwaspadai dalam pengaman informasi ini adalah, berbagai macam virus dan malware. Untuk komputer kita sendiri terdapat 5 level keamanan yakni:

A. Physical Security, yang berfokus pada keamanan fisik device
B. Database dan Devices Security, yang berfokus dalam database mulai dari pembuatannya hingga penerapannya dan devices security yang memastikan bahwa security sistem pada devices tersebut bekerja sebagaimana mestinya.
C. Network Security, yang memastikan keamanan dari segi jaringan seperti firewall, vpn dll.
D. Information Security, yang melindungi informasi sensitive seperti kata kunci, sandi maupun dokumen rahasia
E. Total Security, yang merupakan kombinasi security dari Physical Security hingga information security

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

Jadi menurut saya terkait *Confidentiality, Integrity* dan *Availability (CIA)* yakni:

1.1. Confidentiality (kerahasiaan) yakni data hanya boleh diakses oleh orang yang berhak.

Jadi Confidentiality ini merupakan Upaya menjaga kerahasiaan informasi agar hanya orang, sistem, atau proses yang berwenang yang dapat melihat atau memakainya. Dalam praktiknya, organisasi menerapkan berbagai mekanisme seperti enkripsi, kata sandi yang kuat, autentikasi multi-faktor, serta kebijakan “least privilege” supaya data sensitive misalnya saja rekam medis pasien atau nomor kartu kredit supaya tidak bocor ke pihak yang salah. Tujuannya untuk mencegah pihak yang tidak berwanang atau tak sah mengintip, menyalin, atau menyebarkan isi informasi.

1.2. Integrity (Integritas) yakni data harus tetap akurat dan tidak boleh diubah tanpa izin.

Jadi Integrity menekankan bahwa informasi harus tetap utuh dan akurat, tidak boleh diubah secara tidak sah, baik sengaja maupun karena kesalahan teknis. Untuk menjamin integritas, digunakan teknik seperti hash checksum, tanda tangan digital, kontrol versi, dan audit log, sehingga setiap perubahan bisa dideteksi atau dipulihkan ke keadaan asli. Bayangkan aja kalau isi saldo di rekening bank kita berubah wkwkwk:v jika satu bit saja berubah tanpa prosedur resmi, konsekuensinya bisa fatal maka itulah sebabnya aspek integritas sangat krusial.

1.3. Availability (Ketersediaan) yakni data dan sistem harus selalu bisa diakses oleh pengguna yang berhak

Jadi Availability ini memastikan bahwa data dan layanan selalu siap diakses tepat saat dibutuhkan oleh pengguna yang berhak. Ini dicapai dengan infrastruktur yang andal begitu pula pada server cadangan, koneksi jaringan redundant, sistem pemulihan bencana, dan pemantauan 24 jam serta prosedur teknis seperti load-balancing, fail-over, dan patch rutin. Tanpa ketersediaan, meski data sudah aman dan akurat, manfaatnya hilang; misalnya, layanan mobile banking yang mati ketika nasabah mau transfer akan langsung merugikan bisnis dan menurunkan kepercayaan pengguna.

3. Sebutkan jenis jenis kerentanan keamanan yang anda ketahui !. Solusi:
   Sebenarnya banyak sekali kerentanan yang dapat terjadi dalam upaya mengamankan informasi, jadi saya akan bahas beberapa diantaranya, yakni:

   Mulai dari keamanan fisik dan lingkungan (Physical Security) yakni kadang kali harddisk atau devices sejenisnya terkadang tidak terenskripsi dan mudah dicuri serta beberapa server room pada suatu institut yang tidak terdapat kontrol akses fisik (kayak RFID), CCTV maupun sensor kebakaran. Selain itu kerentanan manusia (Social Engineering) seperti terkena phishing, spear-phising, whaling, Voice Phishing, SMS Phising, baiting (Umpan USB), pretexting, tailgating. Ada juga kerentanan Akun dan identitas seperti keamanan kata sandi lemah atau dia ngambil dari daur ulang password, tidak menggunakan Multi-factor authentification (MFA) dilayanan penting, Privilage escalation karena hak akses terlalu longgar (excessive permissions). Lalu ada juga kerentanan jaringan dan protocol seperti *Man-in-the-middle (MITM)* yakni kita disadap tanpa sadar akan komunikasi kita antara pihak lainnya oleh pihak yang tidak bertanggung jawab, terdapat ASP Spoofing yakni pemalsuan Alamat Media Access Control dari perangkat lain dalam jaringan, Wi-Fi Evil Twin yang Dimana serangan ciber yang memanfaatkan jaringan wi-fi palsu. Selain itu ada juga kerentanan terkait konfigurasi dan infrastruktur yang melibatkan Salah konfigurasi firewall, server, IAM Policy dan sejenisnya maupun TLS/SSL nya lemah yakni protocol lama, cipher suite rentan). Selain itu juga ada kerentanan aplikasi dan kode seperti Insecure Deserialization yaitu sebuah aplikasi web tidak memvalidasi data yang dideserialisasi dengan benar. Dll.

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

   Hash merupakan suatu proses mengubah data (input) menjadi nilai tetap (Output) yang bentukannya unik dan bersifat satu arah Artinya, setelah data diubah menjadi hash, tidak mungkin mengembalikannya ke bentuk aslinya. Fungsi hash digunakan dalam berbagai konteks, seperti penyimpanan password dan integritas data, karena hasilnya selalu sama untuk input yang sama dan berubah total walau ada perubahan kecil pada input. Selain itu,

   Enkripsi adalah proses mengubah data asli (plaintext) menjadi bentuk tidak terbaca (ciphertext) dengan menggunakan algoritma tertentu dan *kunci (key).* Berbeda dengan hash, enkripsi bersifat dua arah yakni, data yang telah dienkripsi dapat dikembalikan ke bentuk aslinya dengan kunci yang sesuai melalui proses dekripsi maupun suatu ketentuan. Enkripsi

digunakan untuk menjaga kerahasiaan data saat dikirim melalui jaringan atau saat disimpan, seperti pada komunikasi WhatsApp, data pada kartu kredit, dan file penting.

Jadi Singkatnya, hash digunakan untuk memastikan data tidak diubah (integritas), sedangkan enkripsi digunakan untuk menjaga data tetap rahasia (kerahasiaan).

5. Jelaskan menurut anda apa itu session dan *authentification!.* Solusi:

   Authentication merupakan proses untuk memverifikasi identitas pengguna. Ketika seseorang login ke sebuah sistem dengan username dan password, sistem akan mengecek apakah kredensial tersebut valid. Jika sesuai, pengguna dianggap "terautentikasi". Authentication biasanya dilakukan satu kali di awal sesi, dan tujuannya adalah memastikan bahwa hanya pengguna yang sah yang bisa mengakses layanan tertentu. Proses ini dapat dilakukan menggunakan berbagai metode, seperti password, kode OTP, sidik jari, atau autentikasi dua faktor (2FA) untuk meningkatkan keamanan.

   Setelah authentication berhasil, sistem akan membuat sebuah session. Session itu sendiri merupakan cara sistem menyimpan informasi sementara tentang pengguna yang sedang aktif, biasanya berupa ID session unik yang dikaitkan dengan pengguna tersebut. ID ini kemudian dikirim ke browser pengguna (biasanya dalam bentuk cookie) dan akan disertakan secara otomatis pada setiap permintaan (request) selanjutnya ke server. Dengan cara ini, pengguna tidak perlu login berulang kali setiap membuka halaman baru. Session akan tetap aktif hingga pengguna logout atau session tersebut kadaluarsa (expired).

   Jadi singkatnya authentication memastikan siapa pengguna itu, dan session menjaga agar pengguna tetap dikenali selama berada di sistem.

6. Jelaskan menurut anda apa itu *privacy* dan ISO !

   Privacy merupakan hak individu atas data pribadinya apalagi di dunia modern ini privasi sangatlah penting dalam menjaga data digital pada setiap individu sehingga tidak dapat digunakan sewenang wenang tanpa suatu perizinan atau persetujuan dari individu yang bersangkutan, sedangkan ISO (International Organization for standardization) merupakan organisasi internasional yang menetapkan standar keamanan di seluruh dunia, biasanya ISO ini untuk memastikan kualitas, keamanan, maupun efisiensi produk, layanan dan sistem di seluruh dunia dengan mengembangkan dan menerbitkan standar global dalam berbagai bidang khususnya keamanan.

STUDI KASUS

Periksalah nim anda misalkan nim anda adalah 20190801067. Silahkan cek digit terakhir apakah berakhiran genap atau ganjil, karena disini berakhiran 7 dan masuk kategori ganjil, maka cek di kategori soal yang ada akhiran7, Sehingga anda mendapat studi kasus TEMA DATA FAKULTAS.

NIM GANJIL		NIM GENAP	
1	Tema Data Kendaraan	0	Tema Data Pembayaran
3	Tema Data Supir	2	Tema Data Pelanggan

5	Tema Data Guru	4	Tema Data Murid
7	Tema Data Fakultas	6	Tema Data Barang
9	Tema Data Beasiswa	8	Tema Data Pasien

Soal:

1. Buatlah solusi teknis dengan menggunakan Framework Laravel 12 dan Filament versi 3 untuk cara penanganan mengamankan data-data tersebut.

Solusi:

Link Github:

https://github.com/Jiwanta384/Keamanan-Informasi_UTS

https://github.com/Jiwanta384/Keamanan-Informasi_UTS.git