Nama: Mahardika

NIM: 20220801441

Matkul: UTS Keamanan Informasi

Dosen: Taufik Rendi Anggara

Jawaban:

No. 1

CIA (Confidentiality, Integrity dan Availability) adalah hal-hal yang dibutuhkan dalam suatu aplikasi.

* Confidentiality adalah kerahasiaan yang harus dimiliki oleh suatu aplikasi, seperti data-data pelanggan yang bersifat rahasia yang tidak boleh diakses atau dimiliki oleh pihak-pihak yang tidak berwenang.
* Integrity adalah integritas suatu aplikasi dalam mengelola data-data pelanggan. Agar data tetap utuh, akurat dan tidak bisa di ubah sembarangan oleh pihak yang tidak berwenang.
* Availability adalah ketersediaan suatu aplikasi harus memastikan bahwa informasi dan system dapat selalu bisa diakses oleh pihak yang berwenang pada saat data tersebut dibutuhkan.

No. 2

Internet

Firewall

Firewall

Jaringan Publik

Jaringan Internal

Tolak jika tidak ada akses / akses tidak sah

Router

Router

Server

Server

Server

Server

Server

Switch Management

Switch Management

No. 3

1. Internet = adalah titik masuk semua aktifitas
2. Firewall = penghalang antara jaringan internal dengan jaringan public yang bertugas untuk mengatur lalu lintas data (dia akan menolak akses yang tidak benar)
3. Router = digunakan untuk menghubungkan jaringan internal dengan internet yang melalui firewall
4. Switch = digunakan untuk menghubungkan server dan perangkat jaringan
5. Server = digunakan untuk berbagai keperluan seperti server aplikasi dan server database yang terhubung ke switch untuk akses dan komunikasi jaringan.

No. 4

Keamanan Perangkat di Remote area seperti BTS sangat sulit untuk dijaga dikarenakan areanya yang tidak berada di lingkungan internal dan tersebar diseluruh titik. Oleh karena itu keamanan fisik dan jaringan sangatlah penting untuk diperhatikan dan di control.

* Keamanan Fisik = pastikan bahwa BTS berada di area yang aman dan dilengkapi dengan system penguncian yang kuat dan berlapis serta berikan tambahan CCTV untuk lebih memudahkan dalam control.
* Keamanan Jaringan = perangkat harus dilengkapi dengan Firewall dan VPN untuk mencegah akses dari pihak eksternal/pihak yang tidak berwenang.

No. 5

Faktor Keamanan yang penting pada Environment Perangkat keras (Hardware).

1. Keamanan Fisik:

Pastikan perangkat ditempatkan dilokasi yang aman dan terlindungi dari akses oleh pihak yang tidak berwenang. Penguncian berlapis, penggunaan CCTV serta kontrol akses terhadap perangkat keras.

1. Keamanan Jaringan:

Perangkat keras harus dilindungi dari ancaman jaringan seperti peretasan, virus, dan serangan DDoS dengan menggunakan firewall, VPN, dan perangkat lunak keamanan.

1. Maintenance dan Patching:

Hardware dan Software harus selalu diupdate dengan versi terbaru untuk mencegah bug dan kerentanan yang terjadi pada hardware dan system

1. Backup dan redudansi:

Untuk memastikan bahwa data selalu tersedia maka kita harus selalu melakukan backup dan redudansi data sehingga jika perangkat keras rusak kita memiliki data-data yang dapat dipulihkan.