RANGKUMAN MODUL 1 CYBER SECURITY, DAN PERBANDINGAN NGINX & APACHE

Tugas Keamanan Jaringan Minggu 1

FEBRUARY 26, 2023

FAJAR YUNUS AFIFFUDIN
NRP 3122640049

Rangkuman Modul 1 : Cyber Security Fundamental

Pada modul ini membahas konsep basic dari cyber security, serta tujuan dan prinsip pada cybersecurity. Selain itu modul ini juga menjelaskan apa yang perlu diamankan pada system.

Pada modul ini berdasarkan sudut pandang dari seorang IT Manager

Internet merupakan jaringan besar dimana terdapat banyak system dan jaringan yang saling terhubung. Sistem yang berbeda dapat saling berinteraksi dengan protocol standar yang mana tiap system dapat saling bertukar informasi satu dengan yang lainnya. Bersamaan dengan ini terdapat juga resiko pada keamanan data.

Jika menyangkut internet, harus memikirkan 3 aspek utama, yakni :

1. Efficiency
2. Reliability
3. Security

Data-data perusahaan sangat berharga, dan merupakan asset bagi suatu perusahaan. Maka data ini perlu diamankan, data dan informasi yang perlu diamankan seperti :

1. Laporan Internal
2. Data Transaksi
3. Data Pelanggan
4. Desain Produk atau rahasia perusahaan

Setelah mengetahui data yang perlu diamankan, perlu tahu beberapa ancaman yang mengancam data tersebut, diantaranya ialah :

1. Unauthorized Modification : Perubahan data yang dilakukan oleh orang yang tidak punya akses
2. Unauthorized Access : Akses informasi oleh orang luar
3. Loss of information : Kehilangan data terjadi ketika informasi berharga atau sensitif di komputer hilang atau tersebar karena pencurian, kesalahan manusia, virus, malware, atau kegagalan daya. Ini juga dapat terjadi karena kerusakan fisik atau kegagalan mekanis atau peralatan suatu bangunan

Data yang perlu diamankan terbagi menjadi 2 golongan data :

1. Data at Rest : Data yang sudah tidak aktif, seperti backup dari aplikasi yan\g sudah off
2. Data Motion : Data yang masih aktif bergerak dan masih dilakukan pengeditan.

Setelah mengetahui data yang perlu diamankan, kita perlu mengetahui tujuan dari pengamanan data tersenbut. Tujuan dari cyber security ini bisa di singkat dengan CIA, dengan detail sebagi berikut ;

C » Confidentally	: dibatasi dari unathorized akses
I » Integrity	: menjaga keakuratan dan kelengkapan informasi (data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi.)
A » Availability	: ketersediaan, informasi bisa diakses oleh orang yang memiliki otoritas kapanpun dan tanpa delay

Studi Kasus :

Contoh penerapan CIA pada webmail

C : Credential hanya diketahui oleh pemilik email, data pasword disimpan dengan enkripsi yang kuat dan tidak mudah untuk di decript

I : Email tidak diubah dari bentuk aslinya

A : Email service harus selalu aktif

Setelah mengetahui tujuan dari cyber security, modul ini membahas kerentanan yang mengancam data. Kerentanan-kerentanan yang mengancam data ialah threat, vulnerabilities, dan risk.

- Threat/ancaman bisa disebabkan secara sengaja ataupun kecelakaan, macam2 jenis ancaman adalah :
  - Natural Threat (bencana alam)
  - Environmental (Lingkungan/ aspek negatif dari aktivitas manusia) = power failure, polusi, liquid leakage (kebocoran / kena air)
  - Human : kelalaian, unathorize access (hancking), virus
- Vulnerability / kerentanan merupakan kekurangan atau kelemahan pada keamanan prosedur system, design, pengimplementasian, dan control dari dalam yang dapat menyebabkan pelanggaran keamanan atau kekerasan pada peraturan keamanan system.
- Risk / resiko adalah hasil yang didapatkan dari kegiatan ancaman dan potensi dari kerentanan informasi yang memberikan dampak pada organisasi

Setelah mengetahui kerentanan data, pada modul ini diberikan cara menanggulangi kerentanan tersebut. Yakni

- Policy & Procedure (Membuat Kebijakan & Prosedur) : Tujuan dari kebijakan dan prosedur adalah untuk membuat semau orang waspada terhadap pentingnya keamanan. Jadi tiap system didefinisikan role dan apa yang bisa dilakukan serta bagian mana saja yang bisa diakses.
- Technical : Tujuan dari technical security control ntuk menangkal serangan luar, seperti virus, ataupun peretas. Yang dilakukan adalah dengan memasang firewall, ids, dan anti virus.
- Phisical : Tujuan dari pengamanan fisik adalah untuk mencegah pencurian, dan penggunaan alat tanpa izin. Yang bisa dilakukan ialah memasng cctv, dan mengamankan dengan kunci

Untuk menerapkan cybersecurity terdapat 2 prinsip yang perlu diingat, yakni

- Principle of Weakest Link : Attacker selalu mencari jalan termudah untuk meretas
- Principle of Least Privilage : Pengguna untuk mengakses perlu izin akses atau authorization

Perbedaan Nginx dan Apache

1. Penanganan Traffic
   Apache : Apache memproses traffic dengan multi-processing modules (MPM)
   Nginx : Web server ini memproses traffic menggunakan algoritma yang bersifat asinkron, non-blocking, dan event-driven
2. Pemrosesan Konten Dinamis
   Apache : Apache bisa memproses konten dinamis tanpa bantuan software tambahan. Hal ini berkat adanya modul yang bisa Anda pasang dan lepas sesuai kebutuhan.
   Nginx : Web server ini bergantung pada adanya software tambahan untuk memproses konten dinamis

ScreenShoot hasil tes pengetahuan modul 1