UHW
UNIVERSITAS HAYAM WURUK
PERBANAS

Pertemuan 15

DASAR KEAMANAN

AUDIO MODUL 15

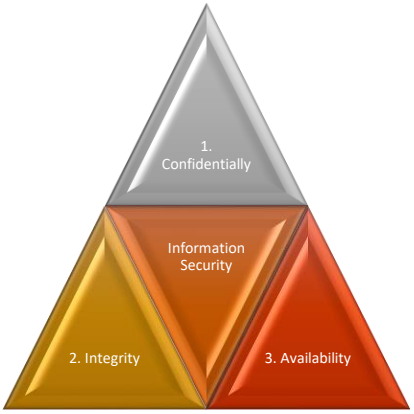
TUJUAN PEMBELAJARAN

Setelah mempelajari bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa mampu menjelaskan bentuk serangan pada jaringan komputer.
2. Mahasiswa mampu menjelaskan keamanan pada topologi jaringan komputer.

CIA TRIAD

Ancaman pada jaringan komputer mempunyai banyak variasi seperti cracker, virus, malware. Dalam bidang keamanan jaringan terdapat aspek CIA Triad yang merupakan aturan dalam mengatur keamanan jaringan dan informasi. CIA merupakan singkatan dari Confidentially, Integrity dan Availability.



Gambar 15. 1 Segitiga CIA

Confidentially (Kerahasiaan) merupakan cara atau usaha untuk menjaga kerahasiaan informasi dengan melakukan pembatasan hak akses dari pengguna yang tidak berwenang.

Integrity (Integritas) yakni menjamin bahwa data yang dikirim dari sumber ke penerima masih terjaga keaslian datanya atau tidak dirubah datanya.

Availability (Ketersediaan) yakni tersedianya informasi ketika dibutuhkan setiap waktu. Artinya sistem harus dalam sistem pertahanan yang baik agar sistem tidak lumpuh.

BENTUK SERANGAN KEAMANAN

Pada jaringan komputer tak terlepas dari serangan oleh phak-pihak yang tidak berwenang. Adapun beberapa bentuk serangan yang terjadi pada jaringan komputer diantaranya:

a. Fabrication: Jenis ini yakni pihak yang tidak mempunyai wewenang berhasil memasukkan pesan-pesan palsu ke jaringan komputer.

b. Interruption: Jenis serangan ini terkait aspek ketersediaan (availability) yang dapat menyebabkan suatu sistem lumpuh atau tidak tersedia untuk diakses. Contoh serangannya adalah denial of service.
c. Interception: Jenis serangan ini berupa penyadapan infromasi oleh pihak yang tidak mempunyai wewenang yang berhasil mengakses data.
d. Modifacation: Jenis serangan ini yakni pihak yang tidak mempunyai wewenang berhasil memodifikasi asset atau data.

KONSEP DASAR JARINGAN KOMPUTER

Keamanan jaringan komputer merupakan satu aspek yang mempunyai peranan sangat penting dalam kaitanynya untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Perangkat-perangkat dalam jaringan komputer harus dilindungi dari segala macam bentuk serangan yang dilakukan oeh pihak-pihak yang tidak mempunyai wewenang. Sistem keamanan dapat berupa dari sisi ekternal, user interface maupun internal. Sistem deteksi yang ada saat ini umumnya mampu mendeteksi adanya jenis serangan yang masuk akan tetapi tidak mampu mengambil tindakan lebih lanjut. Tentu hal tersebut merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis. Apalagi jika sistem pertahanan terhadap sistem masih dilakukan secara manual oleh administrator. Tentu akan mengakibatkan sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespons gangguan yang masuk ke sistem. Hal tersebut dapat berakibat fatal pada sistem mengingat jenis serangan semakin berkembang dan bervariasi. Oleh karena itu perlu dilakukan lang-langkah terkait pengamanan sistem jaringan komputer.

KEAMANAN PADA JARINGAN LAN

Jaringan LAN merupakan jaringan dengan area yang kecil yang biasa diterapkan pada perusahaan, instansi pemerintah maupun di lingkungan pendidikan. Sehingga besar potensinya untuk mendapatkan serangan dari pihak luar. Terdapat beberapa mekanisme dalam mengamankan jaringan LAN.

- FIREWALL

  Merupakan mekanisme sistem keamanan yang diterapkan pada jaringan komputer. Firewall dapat berbentuk hardware atau software yang bertujuan untuk melindungi, baik dengan cara memfilter, membatasi, atau bahkan menolak aktivitas suatu segmen (server, router atau LAN) pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya.
- PORT SECURITY

Jenis keamanan ini dapat diimplementasikan pada perangkat layer 2 yakni Switch. Port security merupakan trafik kontrol yang mendaftarkan dan membatasi perangkat end devices yang dapat terkoneksi ke Switch.

- RADIUS/TACACS Server TACACS (Terminal Access Controller Access-Contol System Server)

  Protokol yang memberikan layanan akses control pada perangkat jaringan seperti router dan switch. Mekanisme ini bekerja dengan sistem terpusat sehingga akan mempermudah dalam pengelolaan authentication, authorization dan accounting. Dengan mekanisme ini network administrator dapat mengganti password pada perangkat jaringan dengan cepat secara terpusat.
- Packet Filtering

  Mekanisme ini bertujuan untuk mengatur lalu lintas paket data dengan cara mengizinkan atau menolak suatu paket data yang melintasi jaringan.

STRATEGI MERANCANG KEAMANAN JARINGAN

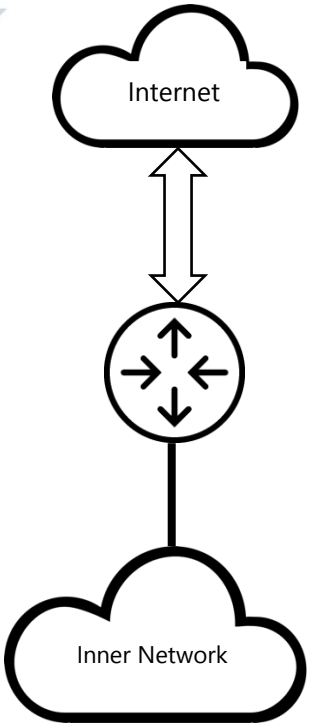
Dalam merancang keamanan jaringan memerlukan strategi dalam mengamankan jaringan agar sistem tidak mudah untuk dimasuki oleh pihak-pihak yang tidak berwenang. Terdapat beberapa strategi yang dapat dilakukan pengelola sistem dalam mengamankan jaringan komputer.

- Hak Akses

  Akses hanya diberikan oleh user yang mempunyai wewenang pada sistem yang ada. Dengan begitu pihak-pihak diluar tidak mudah mengakses sistem pada jaringan.
- Membuat lapisan keamanan

  Pengelola sistem dapat membuat lapisan keamanan dengan beberapa lapisan diantaranya network security, host,/server security dan human security.
- Satu jalur masuk

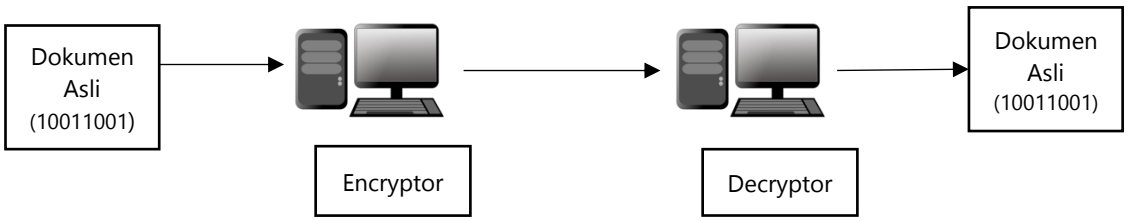
  Keamanan jaringan dapat dengan menggunakan satu jalur masuk yang mana pengelola dapat melakukan monitoring jaringan secara terpusat sehingga akan lebih mudah dalam pengawasannya.



Gambar 15.2 Konsep Satu Jalur Masuk

- Enkripsi data dan digital signature

  Untuk mengamankan data pada jaringan dapat menggunakan enkripsi. Terdapat beberapa metode dalam enkripsi data yang dapat digunakan seperti RSA, MD-5, IDEA, SAFER dll.



Gambar 15.3 Proses Enkripsi dan Dekripsi Data

- Stub Sub Network

  Stub sub network merupakan sebuah strategi yang dapat digunakan untuk mengisolasi sub jaringan yang memerlukan perlindungan secara maksimal dengan membuat hanya satu jalur yang mengarah pada sub jaringan tersebut.

INSTALLASI SISTEM KEAMANAN

Untuk mencegah pihak-pihak yang tidak mempunyai wewenang masuk ke sistem, maka harus dilakukan beberapa langkah untuk mengamankan sistem. Langkah-langkah ini berupa pemasangan hardware maupun software.

- Memasang filter di perangkat router dengan menjalankan fungsi ingrees dan angress filtering.
- Memasang firewall baik berupa hardware dan software. Firewall dapat digunakan untuk memantau lalu lintas pada jaringan, memberikan perizinan paketa yang masuk ke sistem dan memblokir lalu lintas berdasarkan aturan yang ditetapkan.
- Memasang IDS (Intrusion Detection System) dan IPS (Intrusion Prevention Syetem) yang digunakan untuk mendeteksi jika ada paket yang berbahaya.
- Melakukan enkripsi dan autentifikasi. Data yang dikirim dapat dienkrispsi agar tidak mudah untuk dibaca oleh orang-orang yang tidak berwenang serta menggunakan metode autentifikasi sebagai konfirmasi bagi pengguna.

Daftar Pustaka

1. Lukas, J., 2006, Jaringan Komputer, Graha Ilmu, Yogyakarta
2. Sutanta, E., 2005, Komunikasi Data & Jaringan Komputer, Graha Ilmu, Yogyakarta
3. Kurose, Ross, 2017, Computer Networking, A Top-Down Approach (Seventh Edition), Pearson, New York