Keamanan Jaringan

Keamanan Jaringan?

Keamanan jaringan merupakan cara untuk mengamankan jaringan maupun informasi dari pengaksesan, penggunaan, penyingkapan, gangguan, modifikasi, penggandaan dan penghancuran oleh orang yang tidak berhak.

Faktor – Faktor Keamanan Jaringan

Kelemahan manusia (human error)

Kelemahan perangka tkeras komputer

Kelemahan sistem operasi jaringan

Kelemahan sistem jaringan komunikasi

Topics

- The Classic Triad
- Parkerian Hexad
  - Confidentiality
  - Possession
  - Integrity
  - Authenticity
  - Availability
  - Utility
- Fire Wall

C-I-A

CIA atau yang lebih sering disebut CIA Triad merupakan salah satu aturan dasar dalam menentukan keamanan suatu jaringan atau informasi. Parameter dalam CIA ini digunakan untuk menentukan apakah suatu jaringan atau informasi dikatakan aman atau tidak.

Confidentiality

a. **Definisi**: Berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut

b. **Contoh**: data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.

c. **Bentuk Serangan**: usaha penyadapan (dengan program sniffer).

d. **Usaha-usaha:** yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Integrity

a. **Definisi:** informasi tidak boleh diubah tanpa seijin pemilik informasi.

b. **Contoh:** e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.

c. **Bentuk serangan:** Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Availability

a. **Definisi:** berhubungan dengan ketersediaan informasi ketika dibutuhkan.

b. **Contoh:** “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

c. **Bentuk serangan**: Contmailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

Parkerian Hexad

Protect the 6 atomic elements of INFOSEC:

- Confidentiality
- Possession or control
- Integrity
- Authenticity
- Availability
- Utility

Why Parkerian?

Donn B. Parker is a retired (1997) senior management consultant at SRI International in Menlo Park, California who has specialized in Information security and computer crime research for 30 of his 47 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty based on interviews of over 200 computer criminals and reviews of the security of many large corporations.

He received the 1992 Award for Outstanding Individual Achievement from the Information Systems Security Association and the 1994 National Computer System Security Award from U.S. NIST/NCSC, The Aerospace Computer Security Associates 1994 Distinguished Lecturer award, and The MIS Training Institute Infosecurity News 1996 Lifetime Achievement Award.

The Information Security Magazine identified him as one of the five top Infosecurity Pioneers (1998). He formed the International Information Integrity Institute (I-4) at SRI that has been serving over 75 corporate members for 9 years to keep them aware of the most advanced information security concepts and controls.

Confidentiality

- Penjelasan :
  a. Membatasi akses ke sebuah data/informasi yang di anggap penting
  b. Melindungi terhadap pengungkapan yang tidak sah adanya data
- Contoh :
  a. Eksekutif khawatir tentang melindungi rencana strategis perusahaan mereka dari pesaing dan tidak sah ke catatan keuangan mereka.
  b. Catatan kesehatan seseorang disebuah klinik kesehatan yang tidak boleh diungkapkan.

Possession or control

- Penjelasan :
  a. Kontrol atas informasi
  b. Mencegah terjadinya kontak fisik dengan data
  c. Mencegah penyalinan atau penggunan yang tidak sah dari kekayaan intelektual
- Contoh :
  a. Misalkan seorang pencuri yang mencuri amplop tertutup berisi kartu debit bank dan nomor identifikasi pribadi tersebut. Bahkan jika pencuri tidak membuka amplop itu, itu wajar untuk korban menjadi khawatir bahwa pencuri bisa melakukannya setiap saat. Situasi yang menggambarkan hilangnya kontrol atau kepemilikan informasi tetapi tidak melibatkan pelanggaran kerahasiaan.

Integrity

- Penjelasan :
  a. Informasi tidak boleh diubah tanpa seizin pemilik informasi.
  b. Proteksi dilakukan dengan menggunakan signature, certificate atau checksum.
- Contoh :
  a. Bank (Money Bank) untuk menjamin bahwa data tidak bisa ubah atau dimodifikasi oleh pihak-pihak yang tidak berhak atau pihak yang tidak berwenang tanpa seizin dari pemiliknya.

Authenticity

- Penjelasan :
  a. Keaslian atau kebenaran (Authenticity) berkenaan dengan kebenaran atas kepemilikan suatu informasi.

- Contoh :
  a. Ketika kita akan mengakses email kita maka kita akan diminta untuk memasukkan password untuk memastikan bahwa memang kita pemilik dari email account tersebut.
  b. Kita diminta memasukkan PIN setiap kali hendak melakukan transaksi di ATM dan Juga tanda tangan ketika melakukan transaksi di pusat perbelanjaan

Availability

- Penjelasan :
  a. Availability berarti bisa mengakses informasi yang diperlukan kapan saja dan dimana saja.
  b. Menghindari keterlambatan pengaksesan informasi, dan mencegah sistem crash

- Contoh :
  a. Bank yang memiliki layanan internet banking dan ketika nasabah ingin mengakses layanan tersebut ternyata tidak bisa di karenakan layanan tersebut terkena serangan atau dibobol oleh hacker misalnya, hal ini akan menyebabkan mempertanyakan keandalan dan juga kemanan dari layanan internet banking tersebut dan tidak mungkin mereka akan meninggalkan layanan tersebut atau Bahkan kemungkinan nasabah akan pindah ke bank yang bisa memberikan atau menawarkan layanan yang jauh lebih baik

Utility

- Penjelasan :
  a. Utility atau funcionality atau kegunaan.
  b. Bisa juga disimpulkan bahwa informasi itu harus bergunan bagi penerimanya.

- Contoh :
  a. Data seseoarang yang dienkripsi datanya oleh pihak Bank untuk mencegah data tersebut diakses secara tidak sah atau dimodifikasi oleh pihak yang tidak berwenang, akan Tetapi jika pihak bank kehilangan key deskripsinya, maka hal ini akan menyebabkan terjadinya pelanggaran utilitas.
  b. Penggunan mata uang dollar untuk transaksi lokal dirasa kurang tepat.

Exercise - 1

Money Bank adalah sebuah institusi keuangan yang berbasis pada perbankan dengan cabang tersebar di 20 negara. Kegiatan transaksi Money Bank adalah kegiatan via teller, ATM, Internet banking, dan mobile banking. Selama ini perusahaan banyak mendapatkan serangan dari para penyusup dengan berbagai maksud. Selain itu tantangan terbesar adalah bagaimana mengamankan anjungan tunai (ATM) dari para pencuri elektronis.

Exercise - 1

Anda dminta oleh manajemen perusahaan untuk membantu dalam menyelesaikan masalah keamanan dalam sistem elektronik Bank tersebut.

Pertanyaan:

- Jelaskan dalam konteks The Parkerian Hexad elemen-elemen apa saja dalam Money Bank yang harus diproteksi!
- Berikan minimal 5 (lima) kejahatan jaringan 4 tahun terakhir yang terjadi pada bank. Jelaskan secara rinci !

Exercise - 2

Amatilah jaringan di kampusmu. Apakah keamanan jaringannya sudah menerapkan prinsip parkerian hexad? Jika sudah konsep apa saja yang diterapkan? Jika belum konsep apa saja yang harus diterapkan?

TERIMA KASIH