

SECURITY SYSTEM

1. Pengertian

Security system adalah suatu system atau mekanisme yang dirancang sedemikian rupa yang digunakan untuk mengamankan sebuah perangkat hardware atau software pada sebuah computer.

Pada zaman informasi saat ini, kebutuhan teknologi khususnya computer sangat meningkat dari tahun ketahun untuk mempermudah pekerjaan manusia, perkembangan ini juga diikuti dengan beberapa penelitian yang merupakan munculnya pertama kali berkembangnya tindakan criminal informasi yang terjadi pada komputer.

Dari data statistik menunjukkan bahwa serangan computer telah meledak sampai pada worldwide dari tahun ke tahun, yang banyak sangat merugikan si korban, yang mana kejadian ini sangat rentan bagi computer yang terhubung pada suatu jaringan LAN, WAN, dan yang pasti Internet. Si attacker biasanya menyerang suatu system computer yang mempunyai banyak kelemahan dalam proteksi database nya.

Dalam dunia computer, tak ada suatu system pun yang aman 100%, pasti ada setiap kelemahan-kelemahan tertentu yang tersembunyi, yang bisa diexploit. Dan yang hanya bisa dilakukan oleh User adalah untuk meminimalisir setiap kelemahan yang ada pada sebuah computer, oleh karena itu dibutuhkan sebuah system security yang mana telah disediakan oleh banyak developer ataupun vendor-vendor tertentu berupa bayar ataupun gratis.

2. Elemen-Elemen Keamanan Sistem Komputer

a. Vulnerability : Kerentanan

- Sebuah software, hardware atau kelemahan dari prosedur yang menyebabkan penyusup (bisa dikatakan hacker/cracker) dapat membuka celah untuk masuk ke dalam sistem komputer atau jaringan sehingga memiliki kewenangan akses terhadap lingkungan dan sumberdaya yang ada didalamnya.
- Karakteristik dari Vulnerability adalah ke-alpaan atau kelemahan dari penjagaan sehingga sebuah sistem bisa di exploitasi

- Sebuah service yang berjalan di server, atau sistem operasi dikatakan memiliki Vulnerability jika aplikasi didalamnya tidak/belum dilakukan *patch* (update versi) secara berkala
- Terbukanya port pada firewall sebuah server, dan tidak adanya sistem yang mencegah virus masuk (anti virus) pada sebuah komputer dapat dikategorikan sebagai Vulnerability

Threat: Ancaman

- Semua potensi yang membahayakan sistem komputer
- Sebuah threat adalah aktifitas dimana kemungkinan dilakukan oleh seseorang yang akan menidentifikasi atau melakukan eksploitasi terhadap Vulnerability
- Entitas yang mengambil keuntungan dari kerentanan disebut sebagai threat-agent. Seorang threat-agent dapat menjadi seseorang (penyusup) yang mengakses jaringan melalui port pada firewall

Exposure

Sebuah exposure adalah suatu hal yang diexpose oleh threat-agent (hacker/cracker) dan dimungkinkan dapat dibobol

- Vulnerability dari exposure pada sebuah organisasi memungkinkan terjadinya kerusakan sistem
- Contoh dari exposure adalah pada sebuah sistem login dengan user dan password, aplikasi memperbolehkan pembuatan password yang tidak kuat (dimungkinkan password dibuat tanpa kombinasi angka, huruf dan karakter khusus) yang membuat sistem mempunyai celah untuk di susupi oleh hacker/cracker dengan mencoba masuk dengan cara melakukan kombinasi user dan password yang mungkin atau bahkan menangkap informasi dari user yang pernah melakukan login ke sistem

Countermeasure / Safeguard

- Adalah sebuah aplikasi atau software atau hardware atau prosedur yang meminimalkan risiko
- Contohnya Countermeasure : Manajemen password yang kuat dari sistem login, penjagaan keamanan (satpam) pada gedung/ruangan server, mekanisme akses kontrol ke sistem operasi, penggunaan password pada BIOS, training security-awareness

Beberapa hal yang menjadikan kejahatan komputer terus terjadi dan cenderung meningkat adalah sebagai berikut :

1. Meningkatnya pengguna komputer dan internet
2. Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah system dengan cara mencari kelemahan dan celah yang mungkin ada disalahgunakan untuk melakukan scanning system orang lain.
3. Banyaknya software-software untuk melakukan probe dan penyusupan yang tersedia di Internet dan bisa di download secara gratis.
4. Meningkatnya kemampuan pengguna komputer dan internet
5. Desentralisasi server sehingga lebih banyak system yang harus ditangani, sementara SDM terbatas.
6. Kurangnya hukum yang mengatur kejahatan komputer.

3. Macam-macam keamanan atau lingkup security sistem komputer yaitu :

1. Keamanan eksternal / external security

Berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran.

2. Keamanan interface pemakai / user interface security

Berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan

3. Keamanan internal / internal security

Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

2 masalah penting keamanan, yaitu :

1. Kehilangan data / data loss

Yang disebabkan karena :

- Bencana, contohnya kebakaran, banjir, gempa bumi, perang, kerusakan, tikus, dll
- Kesalahan perangkat keras dan perangkat lunak, contohnya ketidak berfungsinya pemroses, disk / tape yang tidak terbaca, kesalahan komunikasi, kesalahan program / bugs.
- Kesalahan / kelalaian manusia, contohnya kesalahan memasukkan data, memasang tape / disk yang salah, kehilangan disk / tape.

2. Penyusup / intruder

- Penyusup pasif, yaitu yang membaca data yang tidak terotorisasi
- Penyusup aktif, yaitu mengubah data yang tidak terotorisasi.

Contohnya penyadapan oleh orang dalam, usaha hacker dalam mencari uang, spionase militer / bisnis, lirikan pada saat pengetikan password.

Sasaran keamanan adalah menghindari, mencegah dan mengatasi ancaman terhadap sistem.

3 aspek kebutuhan keamanan sistem komputer, yaitu :

1. Kerahasiaan / secrecy, diantaranya privasi

Keterjaminan bahwa informasi di sistem komputer hanya dapat diakses oleh pihak-pihak yang terotorisasi

dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem

2. Integritas / integrity

Keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang

terotorisasi

3. Ketersediaan / availability

Keterjaminan bahwa sumber daya sistem komputer tersedia bagi pihak-pihak yang diotorisasi saat diperlukan.

4. Aspek Ancaman Terhadap Security\

Tipe ancaman terhadap keamanan sistem komputer dapat dimodelkan dengan memandang fungsi sistem komputer sebagai penyedia informasi. Berdasarkan fungsi ini, ancaman terhadap sistem komputer dikategorikan menjadi 4 ancaman, yaitu :

1. Interupsi / interruption

Sumber daya sistem komputer dihancurkan / menjadi tak tersedia / tak berguna. Merupakan ancaman

terhadap ketersediaan. Contohnya penghancuran harddisk, pemotongan kabel komunikasi.

2. Intersepsi / interception

Pihak tak diotorisasi dapat mengakses sumber daya. Merupakan ancaman terhadap kerahasiaan. Pihak tak

diotorisasi dapat berupa orang / program komputer. Contohnya penyadapan, mengcopy file tanpa

diotorisasi.

3. Modifikasi / modification

Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya. Merupakan ancaman

terhadap integritas. Contohnya mengubah nilai file, mengubah program, memodifikasi pesan

4. Fabrikasi / fabrication

Pihak tak diotorisasi menyisipkan / memasukkan objek-objek palsu ke sistem. Merupakan ancaman terhadap integritas. Contohnya memasukkan pesan palsu ke jaringan, menambah record file.

Petunjuk prinsip-prinsip pengamanan sistem komputer, yaitu :

1. Rancangan sistem seharusnya publik

Tidak tergantung pada kerahasiaan rancangan mekanisme pengamanan. Membuat proteksi yang bagus

dengan mengasumsikan penyusup mengetahui cara kerja sistem pengamanan.

2. Dapat diterima

Mekanisme harus mudah diterima, sehingga dapat digunakan secara benar dan mekanisme proteksi tidak

mengganggu kerja pemakai dan pemenuhan kebutuhan otorisasi pengaksesan.

3. Pemeriksaan otoritas saat itu

Banyak sistem memeriksa izin ketika file dibuka dan setelah itu (operasi lainnya) tidak diperiksa.

4. Kewenangan serendah mungkin

Program / pemakai sistem harusnya beroperasi dengan kumpulan wewenang serendah mungkin yang

diperlukan untuk menyelesaikan tugasnya.

5. Mekanisme yang ekonomis

Mekanisme proteksi seharusnya sekecil dan sesederhana mungkin dan seragam sehingga mudah untuk verifikasi.

Otentifikasi pemakai / user authentication adalah identifikasi pemakai ketika login.

3 cara otentifikasi :

1. Sesuatu yang diketahui pemakai, misalnya password, kombinasi kunci, nama kecil ibu mertua, dll

Untuk password, pemakai memilih suatu kata kode, mengingatnya dan mengetikkannya saat akan mengakses sistem komputer, saat diketikkan tidak akan terlihat dilayar kecuali misalnya tanda *. Tetapi banyak kelemahan dan mudah ditembus karena pemakai cenderung memilih password yang mudah diingat,

misalnya nama kecil, nama panggilan, tanggal lahir, dll.

Upaya pengamanan proteksi password :

a. Salting, menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai

panjang password tertentu

b. one time password, pemakai harus mengganti password secara teratur, misalnya pemakai mendapat 1

buku daftar password. Setiap kali login pemakai menggunakan password berikutnya yang terdapat pada

daftar password.

c. satu daftar panjang pertanyaan dan jawaban, sehingga pada saat login, komputer memilih salah satu dari

pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.

d. tantangan tanggapan / challenge response, pemakai diberikan kebebasan memilih suatu algoritma

misalnya x3, ketika login komputer menuliskan di layar angka 3, maka pemakai harus mengetik angka 27.

2. Sesuatu yang dimiliki pemakai, misalnya bagde, kartu identitas, kunci, barcode KTM, ATM.

Kartu pengenalan dengan selarik pita magnetik. Kartu ini disisipkan ke suatu perangkat pembaca kartu

magnetik jika akan mengakses komputer, biasanya dikombinasikan dengan password.

3. Sesuatu mengenai / merupakan ciri pemakai yang disebut biometrik, misalnya sidik jari, sidik suara, foto, tanda tangan, dll. Pada tanda tangan, bukan membandingkan bentuk tangannya (karena mudah ditiru) tapi gerakan / arah dan tekanan pena saat menulis (sulit ditiru).

Untuk memperkecil peluang penembusan keamanan sistem komputer harus diberikan pembatasan,

misalnya :

1. Pembatasan login, misalnya pada terminal tertentu, pada waktu dan hari tertentu.
2. Pembatasan dengan call back, yaitu login dapat dilakukan oleh siapapun, bila telah sukses, sistem memutuskan koneksi dan memanggil nomor telepon yang disepakati. Penyusup tidak dapat menghubungkan lewat sembarang saluran telepon, tapi hanya pada saluran tertentu.
3. Pembatasan jumlah usaha login, misalnya dibatasi sampai 3 kali, dan segera dikunci dan diberitahukan keadministrator.

Objek yang perlu diproteksi :

1. Objek perangkat keras, misalnya pemroses, segment memori, terminal, diskdrive, printer, dll
2. Objek perangkat lunak, misalnya proses, file, basis data, semaphore, dll

Masalah proteksi adalah mengenai cara mencegah proses mengakses objek yang tidak diotorisasi. Sehingga dikembangkan konsep domain. Domain adalah himpunan pasangan (objek, hak). Tiap pasangan menspesifikasikan objek dan suatu subset operasi yang dapat dilakukan terhadapnya. Hak dalam konteks ini berarti ijin melakukan suatu operasi.

Cara penyimpanan informasi anggota domain berupa satu matrik besar, dimana :

- Baris menunjukkan domain
- Kolom menunjukkan objek

5. Enkripsi Security Sistem Komputer

4. Definisi Enkripsi

Enkripsi adalah proses mengubah atau mengamankan sebuah teks asli atau teks terangmenjadi sebuah teks tersandi. Dalam ilmu kriptografi, enkripsi adalah proses untukmengamankan sebuah informasi agar informasi tersebut tidak dapat dibaca tanpa pengetahuan khusus.

Contoh penggunaan enkripsi yaitu pada tahun 1970an, dimana enkripsi dimanfaatkan sebagai pengamanan oleh sekretariat pemerintah Amerika Serikat pada domain publik.

Namun sekarang enkripsi digunakan pada sistem secara luas, seperti : ATM pada bank, e-commerce, jaringan telepon bergerak dan lain sebagainya. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman,terutama untuk memastikan integritasdan autentikasi dari sebuah pesan. Contohnya, MessageAuthentication Code(MAC) atau digital signature

Refrensi:

http://yandikofiles.blogspot.com/2009/09/security-system-1_29.html

<http://arisetiabudiblog.wordpress.com/2014/05/25/security-system-komputer/>

<http://rojulman.blogspot.com/2010/06/eleme-elemen-keamanan-sistem-informasi.html>