Jenis – Jenis Ancaman Komputer

1. Virus

Prinsip Virus adalah suatu program yang dapat berkembang dengan menggandakan dirinya. Melalui mekanisme penggandaan diri ini, mekanisme virus digunakan untuk berbagai jenis ancaman keamanan sistem komputer, seperti: menampilkan suatu pesan tertentu, merusak file system, mencuri data, hingga mengendalikan komputer pengguna.Virus dapat menggandakan dirinya melalui email, file-file dokumen dan file program aplikasi.

Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya,yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya.

Suatu program dapat disebut sebagai suatu virus apabila memenuhi minimal 5 kriteria berikut :

1. Kemampuan untuk mendapatkan informasi
2. Kemampuan untuk memeriksa suatu file
3. Kemampuan untuk menggandakan diri dan menularkan diri
4. Kemampuan melakukan manipulasi
5. Kemampuan untuk menyembunyikan diri.

2. Internet Worms

Worm adalah sejenis program yang bisa mengcopy dan mengirim dirinya via jalur komunikasi jaringan Internet. Umumnya menyerang melalu celah/lubang keamanan OS komputer. Worm mampu mengirim paket data secara terus menerus ke situs tertentu via jalur koneksi LAN/Internet. Efeknya membuat trafik jaringan penuh, memperlambat koneksi dan membuat lambat/hang komputer pengguna. Worm bisa menyebar melalui email atau file dokumen tertentu.

3. Spam

Spam adalah sejenis komersial email yang menjadi sampah mail (junkmail). Para spammer dapat mengirim jutaan email via internet untuk kepentingan promosi produk/info tertentu. Efeknya sangat mengganggu kenyamanan email pengguna dan berpotensi juga membawa virus/worm/trojan.

4. Trojan Horse

Trojan adalah suatu program tersembunyi dalam suatu aplikasi tertentu. Umumnya disembuyikan pada aplikasi tertentu seperti: games software, update program, dsb. Jika aktif maka program tersebut umumnya akan mengirim paket data via jalur internet ke server/situs tertentu, atau mencuri data komputer Anda dan mengirimkannya ke situs tertentu. Efeknya akan memenuhi jalur komunikasi, memperlambat koneksi, membuat komputer hang, dan berpotensi menjadikan komputer Anda sebagai sumber Denidal Of Services Attack.

5. Spyware

Spyware adalah suatu program dengan tujuan menyusupi iklan tertentu (adware) atau mengambil informasi penting di komputer pengguna. Spyware berpotensi menggangu kenyamanan pengguna dan mencuri data-data tertentu di komputer pengguna untuk dikirim ke hacker. Efek spyware akan menkonsumsi memory komputer sehingga komputer menjadi lambat atau hang.

6. Sniffing

Pembacaan data yang bukan tujuannya ini dikenal sebagai sniff. Program Sniffer yang digunakan adalah Network Monitor dari Distinct Corporation. Program ini merupakan versi trial yang berumur 10 hari. Di dalam komunikasi TCP/IP atau yang menggunakan model komunikasi 7 layer OSI, sebuah komputer akan mengirim data dengan alamat komputer tujuan. Pada sebuah LAN dengan topologi bus atau star dengan menggunakan hub yang tidak dapat melakukan switch (hub tersebut melakukan broadcast), setiap komputer dalam jaringan tersebut menerima data tersebut. Standarnya hanya komputer dengan alamat yang bersesuaian dengan alamat tujuanlah yang akan mengambil data tersebut. Tetapi pada saat snif, komputer dengan alamat bukan alamat tujuan tetap mengambil data tersebut. Dengan adanya sniffer ini, maka usaha untuk melakukan kriptografi dalam database (dalam hal ini login user dan password) akan sia-sia saja.

Pemberian Hak Akses

Salah satu cara untuk melindungi berkas dalam komputer kita adalah dengan melakukan pembatasan akses pada berkas tersebut. Pembatasan akses yang dimaksudkan adalah kita, sebagai pemilik dari sebuah berkas, dapat menentukan operasi apa saja yang dapat dilakukan oleh pengguna lain terhadap berkas tersebut. Pembatasan ini berupa sebuah permission atau

pun not permitted operation, tergantung pada kebutuhan pengguna lain terhadap berkas tersebut. Di bawah ini adalah beberapa operasi berkas yang dapat diatur aksesnya:

1. Read: Membaca dari berkas
2. Write: Menulis berkas
3. Execute: Meload berkas kedalam memori untuk dieksekusi
4. Append: Menambahkan informasi kedalam berkas di akhir berkas.
5. Delete: Menghapus berkas.
6. List: Mendaftar properti dari sebuah berkas.
7. Rename: Mengganti nama sebuah berkas.
8. Copy: Menduplikasikan sebuah berkas.
9. Edit: Mengedit sebuah berkas.

Selain operasi-operasi berkas diatas, perlindungan terhadap berkas dapat dilakukan dengan mekanisme yang lain. Namun setiap mekanisme memiliki kelebihan dan kekurangan. Pemilihan mekanisme sangatlah tergantung pada kebutuhan dan spesifikasi sistem.

Cara Mengatasi Ancaman Komputer

a. Cara Otentifikasi

- Sesuatu yang diketahui pemakai, misalnya password, kombinasi kunci, nama kecil ibu mertua, dll. Untuk password, pemakai memilih suatu kata kode, mengingatnya dan menggetikkannya saat akan mengakses sistem komputer, saat diketikkan tidak akan terlihat dilaya 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.

b. 4 faktor yang merupakan cara untuk mencegah terjadinya serangan atau kebocoran sistem :

1. Desain sistem : desain sistem yang baik tidak meninggalkan celah-celah yang memungkinkan terjadinya penyusupan setelah sistem tersebut siap dijalankan.
2. Aplikasi yang Dipakai : aplikasi yang dipakai sudah diperiksa dengan seksama untuk mengetahui apakah program yang akan dipakai dalam sistem tersebut dapat diakses tanpa harus melalui prosedur yang seharusnya dan apakah aplikasi sudah mendapatkan kepercayaan dari banyak orang.
3. Manajemen : pada dasarnya untuk membuat suatu sistem yang secure tidak lepas dari bagaimana mengelola suatu sistem dengan baik. Dengan demikian persyaratan good practice standard seperti Standard Operating Procedure (SOP)

dan Security Policy haruslah diterapkan di samping memikirkan hal teknologinya.

4. Manusia (Administrator) : manusia adalah salah satu fakor yang sangat penting, tetapi sering kali dilupakan dalam pengembangan teknologi informasi dan dan sistem keamanan. Sebagai contoh, penggunaan password yang sulit menyebabkan pengguna malah menuliskannya pada kertas yang ditempelkan di dekat komputer. Oleh karena itu, penyusunan kebijakan keamanan faktor manusia dan budaya setempat haruslah sangat dipertimbangkan.

c. Untuk memperkecil peluang penembusan keamanan sistem komputer harus diberikan pembatasan, misalnya :

- Pembatasan login, misalnya pada terminal tertentu, pada waktu dan hari tertentu.
- 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 menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran tetepon tertentu.
- Pembatasan jumlah usaha login, misalnya dibatasi sampai 3 kali, dan segera dikunci dan diberitahukan ke administrator

Sumber

http://yulianakusumawardani.blogspot.co.id/2015/11/ancaman-keamanan-komputer-dan-jaringan.html

https://agilbox.wordpress.com/2015/01/22/ancaman-dan-keamanan-sistem-informasi/

https://alfianurfidiarahmah.wordpress.com/2016/03/25/ancaman-keamanan-pada-sistem-komputer-dan-bagaimana-sistem-operasi-menanganinya/