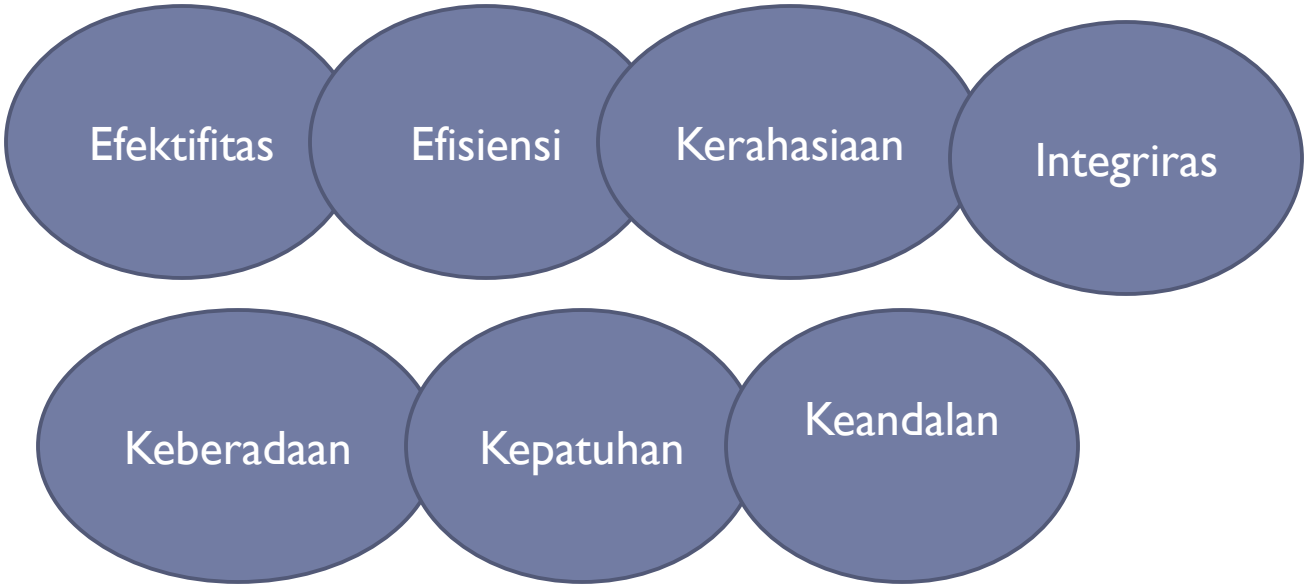
PERTEMUAN 15
KEAMANAN SISTEM INFORMASI

2020

DEFINISI KEAMANAN MENURUT G.J SIMONS

Adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Permasalahan Pokok Sebenarnya Dalam Hal Keamanan Sistem Informasi



DASAR-DASAR DARI KEAMANAN INFORMASI

Tujuan

Menjaga keamanan sumber-sumber informasi , disebut dengan Manajemen Pengamanan Informasi (information security management-ISM) b. Memelihara fungsi-fungsi perusahaan setelah terjadi bencana atau pelanggaran keamanan, disebut dengan Manajemen Kelangsungan Bisnis (business continuity management-BCM).

TUJUAN KEAMANAN INFORMASI MENURUT GARFINKEL

- Kerahasian / privasi
- Ketersediaan/ availability
- Integritas/ integrity
- Autentikasi/ Authentication
- Access Control
- Non-repudiation

KELEMAHAN ANCAMAN

Cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut.

JENIS GANGGUAN / SERANGAN

A. Untuk mendapatkan akses (access attacks)
   Berusaha mendapatkan akses ke berbagai sumber daya komputer atau data/informasi
B. Untuk melakukan modifikasi (modification attacks) Didahului oleh usaha untuk mendapatkan akses, kemudian mengubah data/informasi secara tidak sah
C. Untuk menghambat penyediaan layanan (denial of service attacks) Berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya atau informasi Menghambat penyediaan layanan dengan cara mengganggu jaringan komputer

Beberapa cara dalam melakukan serangan, antara lain:

1. Sniffing➔Memanfaatkan metode broadcasting dalam LAN, membengkokkan aturan Ethernet, membuat network interface bekerja dalam mode promiscuousn. Cara pencegahan dengan pendeteksian sniffer (local & remote) dan penggunaan kriptografi
2. Spoofing➔Memperoleh akses dengan acara berpura-pura menjadi seseorang atau sesuatu yang memiliki hak akses yang valid, Spoofer mencoba mencari data dari user yang sah agar bisa masuk ke dalam sistem. Pada saat ini, penyerang sudah mendapatkan username & password yang sah untuk bisa masuk ke server
3. Man-in-the-middle➔Membuat client dan server sama-sama mengira bahwa mereka berkomunikasi dengan pihak yang semestinya (client mengira sedang berhubungan dengan server, demikian pula sebaliknya)
4. Menebak password

a. Dilakukan secara sistematis dengan teknik brute-force atau dictionary (mencoba semua kemungkinan password)
b. Teknik dictionary: mencoba dengan koleksi kata-kata yang umum dipakai, atau yang memiliki relasi dengan user yang ditebak (tanggal lahir, nama anak, dan sebagainya)

Aspek Ancaman Keamanan Komputer Atau Keamanan Sistem Informasi

1. INTERRUPTION
2. INTERCEPTION
3. MODIFICATION
4. FABRICATION

RESIKO

Dengan mengetahui ancaman dan kelemahan pada sistem informasi terdapat beberapa kriteria yang perlu diperhatikan dalam masalah keamanan sistem informasi yang dikenal dengan 10 domain, yaitu :

1. Akses kontrol sistem yang digunakan
2. Telekomunikasi dan jaringan yang dipakai
3. Manajemen praktis yang di pakai
4. Pengembangan sistem aplikasi yang digunakan
5. Cryptographs yang diterapkan
6. Arsitektur dari sistem informasi yang diterapkan
7. Pengoperasian yang ada
8. Busineess Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
9. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan
10. Tata letak fisik dari sistem yang ada

Macam-macam resiko

1. Pengungkapan dan pencurian
2. Penggunaan secara tidak sah
3. Pengrusakan secara tidak sah dan penolakan pelayanan
4. Modifikasi secara tidak sah

PENGENDALIAN

1. Kontrol administratif
2. Kontrol Pengembangan dan Pemeliharaan Sistem
3. Kontrol Operasi
4. Proteksi Fisik terhadap Pusat Data Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar.
5. Kontrol Perangkat Keras

6. Kontrol Akses terhadap Sistem Komputer
7. Kontrol terhadap akses informasi
8. Kontrol terhadap bencana
9. Kontrol terhadap perlidungan terakhir
10. Kontrol Aplikasi

Metodologi Keamanan Sistem Informasi

1. Keamanan level 0, keamanan fisik
2. Keamanan level 1, meliputi database, data security keamanan dari PC itu sendiri, device, dan application.
3. Keamanan level 2, Keamanan Network security
4. Keamanan level 3, Menyangkut information security,

CARA MENDETEKSI SUATU SERANGAN

1. Desain sistem
2. Aplikasi yang dipakai
3. Manajemen
4. Manusia (administrator)

Strategi Dan Langkah Pengamanan

1. Keamana fisik
2. Kunci komputer
3. Keamanan BIOS
4. Mendeteksi gangguan keanmanan fisik

Langkah Keamanan Sistem Informasi

1. Aset
2. Analisa resiko
3. Perlindungan
4. Alat
5. Prioritas

Upaya Melindungi Sistem Informasi

1. Pendekatan preventif yang bersifat mencegah dari kemungkinan terjadinya ancaman dan kelemahan
2. Pendekatan detective yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal
3. Pendekatan Corrective yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

TERIMAKASIH