NIM : 1310651139

NAMA : YANI FATHUR RAHMAN

KELAS : B

DOMAIN 1: ACCES CONTROL

KONSEP CORNERSTONE DALAM KEAMANAN INFORMASI DALAM 10 DOMAIN

Tiga konsep utama dalam sebuah konsep keamanan CIA adalah

Confidenlity (kerahasiaan) adalah sebuah informasi dari sebuah data rahasia, dengan kata lain kerahasiaan adalah sebuah pencegahan terhadap akses yang tidak sah membaca data, contoh pencurian data kerahasiaan adalah pencurian data pada credit card.

Integrity (integritas) adalah sebuah pencegahan terhadap sebuah perubahan data dan intergritas merubah terjadi perubuhan tulisan pada data.

Avilability (ketersediaan) adalah memastikan bila sitem tersebut di perlukan dan system tersebut harus bias digunakan, contoh serangan dalam sebuah ketersediaan adalah DOS (denial-of-service) penolakan sebuah akses terhadap sebuah data.

Dalam konsep CIA triad juga dijelaskan oleh kebalikannya : Disclosure, Alteration, Destruction (pengungkapan,perubahan,penghapusan) pengungkapan adalah sebuah pengukapan informasi yang tidak sah, perubahan adalah sebuah perubahan terhadap sebuah data, dan penghapusan membuat data tidak tersedia. Dalam sistem CIA terkadang di rubah menjadi DAD

Identity and authentication, authorization, and accountability

Identity and authentication adalah sebuah indentitas dan otentikasi dalam mengklaim dalam mengkalim sebuah indentitas seseorang, contoh apa bila ada orang lain mengklaim dan apa bila ornag tersebut tidak mempunyai bukti, ada juga orang lain yang mengklaim tetepi orang tersebut mempunyai bukti dan buti tersebutlah yang menjadi password.

Authorization adalah otoritas menjelaskan tentang apa yang anda perbuat terhadap satu system identifikasi tindakan terseut termasuk membaca, menulis, dan mengeksekusi sebuah file dalam sebuah program.

Accountability adalah akuntabilitas merupakan sebuah tindakan dengan menganalisa danmasuk untuk mengaudit data, menegakan akuntabilitas mampu menjaga pengguna dan mengetaui data login tidak cukup untuk memberikan sebuah audit terhadap sebuah akuntabilitas.

Nonrepudiation adalah penolakan penyangkalan pengguna terhadap sebuah transaksi.

Least privilege and need to know adalah pemberian minimum akses terhadap sebuah akses untuk mencegah keluarnya sebuah informasi.

Subjects and objects adalah pemberian sebuah entitas system data yang aktif, dan objek adalah sebuah data pasih yang terdapat dalam seuah system.

Defense-in-depth adalah sebuah pertahan berlapais dalam sebuah data dan informasi, dan pertahan berlapis tersebut dapat digunakan untuk keamanan dalam sebuah data.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

Kategori akses control dan tipe dalam sebuah system keamanan dan setiap jenis keamanan berbeda-beda dalam sistemnya, ada 6 tipe kemanan :

• Preventive

Control pencegahan, dan memberi pembatasan terhadap pengguna

• Detective

Control yang selalu siaga setelah terjadinya serangan dan sebelum terjadinya serangan

• Corrective

Control yang bekerja memperbaiki system atau proses yang rusak

• Recovery

Control pemulih setelah insiden keamanan terjadi

• Deterrent

Control yang selalu waspada terhadap sebuah serangan yang akan terjadi maupun sudah terjadi

• Compensating

Control tambahan yang dimasukan untuk mengimbangai control yang lain

ACCESS CONTROL TECHNOLOGIES

Single sign-on

Single sign-on memungkinkan sebuah system mengontetifikasikan sekali dan setelah itu dapat di gunakan untuk mengakses beberapa system dan hal ini memungkinkan admin untuk menambah dan mengganti dan mencabut hak user