INFORMATION ASSURANCE AND SECURITY

Keamanan informasi, Cara dari kita untuk berusaha mengantisipasi kemungkinan adanya kejahatan cyber seperti, pencurian informasi, scam, dan lain sebagainya, Karena di era digital ini hal yang paling penting dari semua itu adalah data dari seseorang yang bisa saja digunakan oleh orang – orang yang tidak bertanggung jawab untuk hal – hal yang bisa merugikan pihak yang memiliki informasi tersebut, Tujuan dari pembelajaran Keamanan Sistem Informasi:

* Penjaminan Integritas Informasi
* Pemastian Kesiagaan Sistem Informasi
* Pengamanan Kerahasiaan Data
* Pemastian Memenuhi Peraturan, Hukum dan Bakuan yang berlaku

Dalam pembelajaran Keamanan informasi, terdapat juga aspek – aspek dari Keamanan Sistem Informasi itu sendiri, menurut seorang pakar bernama *Garfinkel “Keamanan komputer meliputi Privacy, Integrity, Authentication dan availability”*. Pemaparan mengenai 4 aspek yang disampaikan Garfinkel seperti ini:

* Privacy / Confidentiality
* Integrity
* Authentication
* Availability
* Non-Repudiation

Ancaman dalam keamanan komputer / keamanan sistem informasi pun ada, terdapat beberapa ancaman seperti:

* Interruption (Informasi yang tersimpan di suatu database dirusak atau dicuri sehingga tidak bisa digunakan lagi)
* Interception (Informasi yang dimiliki seseorang bisa disadap seseorang bisa masuk ke dalam device target tanpa diketahui)
* Modifikasi (Dapat mengubah dan memanipulasi data yang sedang dikirimkan seseorang)
* Fabrication (Seseorang dapat meniru informasi dari suatu orang kemudian, informasi yang mereka dapatkan, bisa diarahkan kepada orang – orang terdekat dari orang yang mereka tiru, seperti melakukan penipuan dan lain – lain)

Metodologi (Tingkatan) Keamanan sistem Komputer, terdapat beberapa tingkatan dari Keamanan sistem Komputer seperti:

* Keamanan Level 0 (Paling bawah / basic, jika ini bobol, maka data bahkan hardware pun tidak bisa dilindungi)
* Keamanan Level 1 (Tingkat lebih tinggi dari 0, berkaitan dengan Database, data security, Keamanan Pc itu sendiri dll)
* Keamanan Level 2 (Berkaitan dengan keamanan jaringan yang tersambung dengan perangkat / device user)
* Keamanan Level 3 (Berkaitan dengan keamanan informasi dari user itu sendiri, seperti password dan lain – lain)
* Keamanan Level 4 (Ini merupakan keamanan gabungan dari seluruh level sebelumnya, jika semua level sebelumnya berjalan dengan baik maka level ini bisa terpenuhi)

Ada juga cara untuk bisa mendeteksi suatu serangan atau kebocoran sistem yang harus dilihat seperti:

* Desain sistem (Jika sistem di desain dengan baik, harusnya tidak meninggalkan celah sedikit pun)
* Aplikasi yang dipakai (Aplikasi yang digunakan harus dilihat apakah, mendapat banyak feedback positif dari user lain)
* Manajemen (Sistem harus dikelola dengan sangat baik)
* Manusia (Dalam perancangan suatu sistem pun harus memerhatikan kemampuan user itu sendiri sebagai pengguna dan harus mudah digunakan)

Langkah keamanan sistem informasi, seperti:

* Aset (Perancangan keamanan aset dari user harus benar – benar diperhatikan)
* Identifikasi resiko (Menghitung dan mengantisipasi resiko apa saja yang kemungkinan terjadi dalam penggunaan sistem ini)
* Perlindungan (Penggunaan Internet Firewall dalam melindungi jaringan internet)
* Alat (Alat yang digunakan harus dipastikan benar – benar aman)
* Prioritas (Dalam hal ini keamanan jaringan komputer merupakan suatu prioritas)