

Nama : Syifa Azzahra

NIM : 24060118130149

UAS Keamanan Jaringan dan Komputer (Rabu, 9 Juni 2021)

1. Terkait Keamanan dan Jaminan Informasi, kita mengenal istilah kerentanan dan ancaman. Sebut dan jelaskan klasifikasinya masing-masing! Berikan contohnya masing-masing!

Jawaban :

Klasifikasi Kerentanan :

1. **Jenis tindakan (type action)** yang menyebabkan kerentanan untuk memanifestasikan dirinya: tindakan disengaja (atau tidak bertindak) atau tindakan jahat disengaja atau tidak bertindak.
Contoh : penghapusan data
2. **Metode Eksploitasi kerentanan** yaitu keterlibatan pelaku baik langsung atau tidak langsung pada bagian tertentu.
Contoh : mengeksploitasi data – data
3. **Sifat dari kerentanan atau kelemahan (type kerentanan)** yaitu keselamatan, keandalan, keamanan, atau beberapa kombinasi daripadanya.
Contoh : tidak amannya suatu data

Klasifikasi Ancaman :

1. **Ancaman aktif** merupakan suatu kejahatan yang terjadi pada komputer dan suatu kecurangan berupa pencurian data.
Contoh : memodifikasi data
2. **Ancaman pasif** merupakan kegagalan sistem itu sendiri atau kesalahan manusia dalam memproses sistem, atau karena adanya bencana alam yang terjadi yang mengakibatkan ancaman bagi sistem itu sendiri
Contoh : bencana alam, kesalahan manusia (kesalahan memasukkan data dan penghapusan data), kegagalan sistem.

2. Deskripsikan kronologi dalam penerapan pengukuran kendali atas ancaman pada Keamanan dan Jaminan Informasi?

Jawaban :

- a. Anticipate prevent antara lain IA analysis technique, IA integrity level, IA design technique/features, Perception managemen □ Melakukan antisipasi terlebih dahulu sebelum melakukan pengukuran kendali atas ancaman.
 - b. Detect antara lain IA design technique/ features, in service considerations, operational procedures □ Melanjutkan dengan mendeteksi dalam pengukuran kendali ancaman.
 - c. Characterize antara lain IA analysis technique, controllability, IA accident/incident investigation technique □ Setelah dilakukan pendektasian melakukan karakteristik ancaman nya seperti apa.
 - d. Respond, contain consequence antara lain IA design technique/ features, operational procedures, contingency plans □ Merespon ancaman yang masuk dari hasil karakteristik nya.
 - e. Recover antara lain operational procedures, contingency plans □ Ancaman tersebut kemudian dilakukan pemulihan.
3. Sebutkan kegiatan apa saja yang terlibat dalam memverifikasi efektivitas pengukuran pengendalian ancaman terhadap Jaminan informasi?

Jawaban :

- Tindakan pengendalian tergantung pada ketelitian analisis eksposur risiko yang mendahuluinya.
 - Eksposur risiko ditentukan dan ditinjau secara bertahap:
 1. Paparan risiko awal dipastikan untuk memprioritaskan tindakan pengendalian ancaman.
 2. Tindakan pengendalian ancaman dilaksanakan sesuai dengan prioritas ini.
 3. Efektivitas tindakan pengendalian ancaman (siswa risiko eksposur) diverifikasi.
4. Misalkan Anda mengunjungi situs web e-commerce seperti bank Anda, saham broker, dll. Sebelum Anda mengetikkan informasi yang sangat sensitif, Anda ingin memiliki beberapa jaminan bahwa informasi Anda akan dilindungi. Apakah Anda (Memiliki jaminan seperti itu)? Bagaimana kau bisa tahu? Hal-hal yang relevan dengan keamanan

apa yang ingin Anda terjadi, atau tidak terjadi ketika Anda menggunakan situs web seperti itu?

Jawaban :

Keinginan saya jika terjadi hal hal yang diluar kendali bank dan saya, pihak bank tentu harus ebrtanggung jawab dan melaksanakan kewajibannya sebagaimana yang telah tertuang pada kesepakatan yang telah dibuat.

Hal yang bukan keinginan saya antara lain seperti mengirimkan permohonan yang tidak diinginkan, Tidak memantau aktivitas internet konsumen tanpa izin dan tidak mengalihkan informasi pribadi ke pihak ketiga.