NO :1

Disini saya akan me resume tentang Operations Security. Terdapat 5 poin yang akan saya bahas di Operations Security, yaitu :

1. Administrative Security
2. Sensitive Information/Media Security
3. Asset Management
4. Continuity of Operations
5. Incident Response Management

ADMINISTRATIVE SECURITY

Aspek fundamental dari Administrative security adalah sebagai kontrol kepada masyarakat baik sengaja maupun tidak disengaja dalam mengorbankan kerahasiaan, integritas, dan ketersediaan data dalam sebuah sistem. Disini juga disediakan sarana untuk mengontrol operasional akses data.

Dari segi label, keamanan informasi dibagi menjadi 3 bagian, yaitu :

1. Top secret : untuk data yang yang sangat rahasia, seperti laporan intelijen negara.
2. Secret : untuk data yang rahasia, seperti operasi rahasia yang dilakukan oleh negara.
3. Confidential : untuk data yang bisa menyebabkan ancaman kepada keamanan nasional, seperti terorisme.

Sistem label diatas juga diterapkan pada perusahaan swasta, tetapi untuk perusahaan swasta menggunakan label “Internal Use Only” dan “Company Proprietary”.

Administrative security juga harus memenuhi beberapa persyaratan, seperti :

1. **Clearance :** penggunaan izin disini dibagi menjadi beberapa tingkat dan penggunaan izin sendiri ditentukan oleh subyek, seperti penyalahgunaan narkoba dsb. Untuk tingkatan yang lebih tinggi digunakan metode Compartmentalization.
2. **Separation of duties :** digunakan oleh seseorang yang hanya memiliki akses istimewa, dan diantara mereka tidak ada yang memiliki kontrol secara total terhadap suatu transaksi data.
3. **Rotation of duties :** digunakan oleh sebuah organisasi untuk merotasi staf dan juga untuk menghindari kebocoran data.
4. **Mandatory leave/forced vacation :** hal ini diambil dengan pertimbangan keamanan sebagai dasar, dan untuk mengurangi atau mencegah penipuan data di internal organisasi.
5. **Nondisclosure agreement :** perjanjian disini diambil untuk menjaga kerahasiaan data dan disepakati oleh internal organisasi.
6. **Background checks :** merupakan kontrol direktif tambahan yang dilakukan oleh sebuah organisasi untuk mengurangi tingkat kejahatan yang akan terjadi di dalam organisasi.

SENSITIVE INFORMATION/MEDIA SECURITY

Pada bagian ini akan membahas tentang komponen-komponen penting dari keseluruhan keamanan informasi.

1. **Labeling/marking :** merupakan langkah terpenting dalam menjaga informasi sensitif.
2. **Handling :** informasi sensitif ditangani oleh seseorang dalam internal organisasi dengan kebijakan penanganan yang ketat.
3. **Storage :** penggunaan metode enkripsi dalam menyimpan informasi sensitif.
4. **Retention :** pada bagian ini lebih menekankan pada media penyimpanannya.
5. **Media sanitization or destruction of data :** dalam proses ini terdapat beberapa metode untuk melakukannya, yaitu :
    - Data remanence
    - Wiping, overwriting, dan shredding
    - Degaussing
    - Phisycal destruction
    - Shredding

ASSET MANAGEMENT

Pada poin ini lebih menekankan pada fokus pada orang, data, dan media penyimpanan dalam keamanan informasi. Pada poin ini akan dibahas tentang manajemen konfigurasi. Manajemen konfigurasi sendiri terdiri dari beberapa tipe, yaitu :

1. **Baselining :** konfigurasi yang menangkap titik dalam sistem keamanan informasi.
2. **Vulnerability management :** diterapkan dalam pencarian patch yang hilang pada komponen data.
3. **Change management :** terdapat beberapa langkah untuk mengubah manajemen, yaitu :

    a. Mengidentifikasi perubahan
    b. • Mengusulkan perubahan
    c. • Menilai risiko yang terkait dengan perubahan
    d. • Pengujian perubahan
    e. • Penjadwalan perubahan
    f. • Memberitahukan pihak yang terkena dampak dari perubahan
    g. • Menerapkan perubahan
    h. • Hasil Pelaporan pelaksanaan perubahan

CONTINUITY OF OPERATIONS

Pada poin ini akan membahas tentang operasi yang berkelanjutan. poin ini lebih menekankan pada kerahasiaan, integritas, dan ketersediaan triad.

1. **Service level agreements :** menekankan pada aspek tanggung jawab organisasi dalam pemberian penyediaan layanan serta kualitas layanan.
2. **Fault tolerence :** terdiri dari beberapa aspek, yaitu :
    - Backup
    - Redundant array and inexpensive disk

- Systems redudantcy

INCIDENT RESPONSE MANAGEMENT

Poin ini membahas tentang manajemen tindakan yang akan dilakukan bila terjadi insiden pada sebuah data. Terdapat enam langkah siklus hidup respon insiden, yaitu :

1. **Preparation**
2. **Detection and analysis**
3. **Containtment**
4. **Eradication**
5. **Recovery**
6. **Lesson learned**

Selain itu, terdapat serangan lain yang berupa malware. Berikut daftar beberapa jenis malware :

Table 7.2 Types of Malware

Malicious Code	Description
Virus	A *virus* is malware that does not self propagate: it requires a carrier, such as a human manually moving an infected USB device from one system to another
Macro virus	A *macro virus* is malware that infects Microsoft Office documents by means of embedding malicious macros within them
Worm	A *worm* is malware that self-propagates. Some of the most well-known names of malware fall under the worm category: Code Red, Nimda, SQL Slammer, Blaster, MyDoom, and Witty
Trojan Horse	*A Trojan Horse* is malware that has two functions: one overt (such as a game) and one covert (such as providing an attacker with persistent backdoor access)
Rootkit	A *rootkit* is malware that violates system integrity and is focused on hiding from system administrators. Typical capabilities include file, folder, process, and network connection hiding

DoS Name	Type	Description
Land	Malformed packet	The *land attack* uses a spoofed SYN packet that includes the victim's IP address as both source and destination
Smurf	Resource exhaustion	A *Smurf attack* involves ICMP flooding. The attacker sends ICMP Echo Request messages with spoofed source addresses of the victim to the directed broadcast address of a network known to be a Smurf amplifier. A Smurf amplifier is a public-facing network that sends a large number of responses from traffic sent to directed broadcast addresses
SYN Flood	Resource exhaustion	A *SYN Flood* sends many TCP packets with the SYN flag set to a victim and ignores the victim's SYN/ACK packets. The victim's half-open connection queue may eventually fill and be unable to process new connections
Teardrop	Malformed packet	The *teardrop attack* sends packets with overlapping fragment offsets, which may crash the system that is attempting to reassemble the fragments
Ping of Death	Malformed packet	The *Ping of Death* sends fragmented ICMP Echo Requests that, once reassembled, are larger than the maximum size of an IP packet
Fraggle	Resource exhaustion	The *Fraggle attack* is a variation of the Smurf attack. While Smurf uses ICMP, fraggle uses UDP
DNS reflection		A *DNS reflection attack* sends high numbers of DNS requests spoofed from the victim to publicly accessible recursive DNS name servers

NO. 2

STUDI KASUS

MOSCOW - Lebih dari 100 ribu situs WordPress dilaporkan terinfeksi dengan malware jenis baru. Malware asal Rusia ini disebut dengan nama SoakSoak dan telah ditemukan sejak September 2014.

Dilansir *Itproportal*, Selasa (16/12/2014), malware Rusia ini kabarnya memanfaatkan kesalahan dalam *plug-in slideshow* yang dinamakan Slider Revolution. Tim di belakang*plug-in* telah mengetahui kecacatan tersebut sejak September, tetapi tidak ada yang dapat dilakukan untuk memberantas masalah ini.

Menurut perusahaan riset di Sucuri, Google telah memblokir 11 ribu domain yang terinfeksi. Akan tetapi, kabarnya ada lebih banyak situs yang belum diketahui bahwa sesungguhnya mereka terinfeksi malware.

Menjadi sulit untuk mencegah penyebaran malware. Untuk bisa menghapus ancaman secara penuh, plug-in premium harus diperbarui yang bisa diselesaikan secara manual oleh situs administrator.

Dulfy, sebuah website video game telah sukses menghapus kode berbahaya dan sekarang telah menerapkan firewall. Namun, pemilik situs masih percaya bahwa ancaman itu kemungkinan bisa datang kembali.

Serangan SoakSoak memiliki potensi untuk menyebabkan kerusakan besar pada sistem manajemen konten WordPress. Pengguna yang mengunjungi situs yang terinfeksi dianggap berisiko, yang dikhawatirkan dapat menyebarluaskan malware tersebut.