Jawaban No.1

Sistem Informasi Manajemen- Keamanan Informasi

Pengertian Keamanan Informasi

Keamanan Informasi atau Information Security adalah proteksi peralatan computer, fasilitas, data, dan informasi, baik computer maupun non-komputer dari penyalahgunaan oleh pihak-pihak yang tidak terotorisasi/ tidak berwenang.

Tujuan Keamanan Informasi:

1. Kerahasiaan
   Perusahaan berusaha untuk melindungi data dan informasinya dari pengungkapan kepada orang-orang yang tidak berwenang.
2. Ketersediaan
   Perusahaan menyediakan data dan informasi yang tersedia untuk pihak-pihak yang memiliki wewenang untuk menggunakanannya.
3. Integritas
   Semua system informasi harus memberikan representasi akurat atas system fisik yang direpresentasikannya.

Manajemen Keamanan Informasi (Information Security Management)

Merupakan aktivitas untuk menjaga agar sumber daya informasi tetap aman.Manajemen tidak hanya diharapkan untuk menjaga sumber daya informasi aman, namun juga diharapkan untuk menjaga perusahaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan.

Tahapannya yaitu:

1. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
2. Mendefinisikan risiko yang dapat disebabkan oleh ancaman-ancaman tersebut.
3. Menentukan kebijakan keamanan informasi.
4. Mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut

Strategi dalam ISM:

1. Manajemen Risiko (Risk Management)
   Dibuat Untuk menggambarkan pendekatan dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.
2. Tolak Ukur
   Adalah tingkat keamanan yang disarankan dalam keadaan normal harus memberikan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi.

Ancaman Keamanan Informasi (Information Security Threat)

Merupakan orang, organisasi, mekanisme, atauperistiwa yang memiliki potensi untuk membahayakansumber daya informasi perusahaan.

1. Ancaman Internal

Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut.

2. Ancaman Eksternal

Misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan kita atau disebut juga pesaing usaha.

Jenis- Jenis Ancaman:

Malicious software, atau malware terdiri atas program-program lengkap atau segmen-segmen kode yang dapat menyerang suatu system dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemilik system.

Peranti Lunak yang berbahaya (Malicious Software-Malware)
1. Virus Adalah program komputer yang dapat mereplikasi dirinya sendiri tanpa dapat diamati oleh si pengguna dan menempelkan salinan dirinya pada program-program dan boot sector lain
2. Worm Program yang tidak dapat mereplikasikan dirinya sendiri di dalam sistem, tetapi dapat menyebarkan salinannya melalui e-mail
3. Trojan Horse Program yang tidak dapat mereplikasi atau mendistribusikan dirinya sendiri, namun disebarkan sebagai perangkat
4. Adware Program yang memunculkan pesan-pesan yang mengganggu
5. Spyware Program yang mengumpulkan data dari mesin pengguna

Risiko Keamanan Informasi (Information Security Risk)

Didefinisikan sebagai potensi output yang tidak Diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Risiko-risiko seperti ini dibagi menjadi empat jenis yaitu:

- **Interuption:ancaman terhadap availability, yaitu data dan informasi yang berada dalam system computer yang dirusak dan dibuang sehingga menjadi tidak ada atau menjadi tidak berguna.**
- **Interception: merupakan ancaman terhadap secrey, yaitu orang yang tidak berhak mendapatkan akses informasi dari dalam system computer**
- **Modification: merupakan ancaman terhadap integritas, yaitu orang yang tidak berhak, tidak hanya berhasil mendapatkan akses, melainkan juga dapat melakukan pengubahan terhadap informasi.**
- **Fabrication: adanya orang yang tidak berwenang, meniru atau memalsukan suatu objek ke dalam system.**

Manajemen Risiko (Management Risk)

Manajemen Risiko merupakan satu dari dua strategi untuk mencapai keamanan informasi.Risiko dapat dikelola dengan cara mengendalikan atau menghilangkan risiko atau mengurangi dampaknya.

Tingkat keparahan dampak dapat diklasifikasikan menjadi:

1. dampak yang parah (severe impact) yang membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan tersebut untuk berfungsi
2. dampak signifikan (significant impact) yang menyebabkan kerusakan dan biaya yang signifikan, tetapi perusahaan tersebut tetap selamat
3. dampak minor (minor impact) yang menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

Tabel Tingkat Dampak dan Kelemahan

	Dampak Parah	**Dampak Signifikan**	**Dampak Minor**
Kelemahan Tingkat Tinggi	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Menengah	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Rendah	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Analisis kelemahan tidak dibutuhkan

Serangan-serangan dalam Keamanan Informasi

1. Serangan untuk mendapatkan akses

Caranya antara lain: Menebak password, terbagi menjadi 2 cara:

a. Teknik mencoba semua kemungkinan password
b. Mencoba dengan koleksi kata-kata yang umum dipakai. Missal: nama anak, tanggal lahir

2. Serangan untuk melakukan modifikasi

Setelah melakukan serangan akses biasanya melakukan sesuatu pengubahan untuk mendapatkan keuntungan. Contoh:

a. Merubah nilai
b. Penghapusan data hutang di bank

3. Serangan untuk menghambat penyediaan layanan

Cara ini berusaha mencegah pihak-pihak yang memiliki pemakai sah atau pengaruh luas dan kuat untuk mengakses sebuah informasi

Missal:

a. Mengganggu aplikasi
b. Mengganggu system
c. Mengganggu jaringan

Kebijakan Keamanan Informasi

Suatu kebijakan keamanan harus diterapkan untuk mengarahkan keseluruhan program. Perusahaan dapat menerapkan keamanan dengan pendekatan yang bertahap, diantaranya:

a. Fase 1:

Inisiasi Proyek. Membentuk sebuah tim untuk mengawas proyek kebijakan keamanan tersebut.

b. Fase 2:

Penyusunan Kebijakan. Berkonsultasi dengan semua pihak yang berminat dan terpengaruh.

c. Fase 3:

Konsultasi dan persetujuan.Berkonsultasi dengan manajemen untuk mendapatkan pandangan mengenai berbagai persyaratan kebijakan.

d. Fase 4:

Kesadaran dan edukasi.Melaksanakan program pelatihan kesadaran dan edukasi dalam unit-unit organisasi.

e. Fase 5:

Penyebarluasan Kebijakan. Kebijakan ini disebarluaskan ke seluruh unit organisasi dimana kebijakan tersebut dapat diterapkan.

Kebijakan Keamanan yang Terpisah

Keamanan Sistem Informasi
Pengendalian Akses Sistem
Keamanan Personel
Keamanan Lingkungan Fisik
Keamanan Komunikasi data
Klasifikasi Informasi
Perencanaan Kelangsungan Usaha
Akuntabilitas Manajemen

kebijakan terpisah ini diberitahukan kepada karyawan, biasanya dalam bentuk tulisan, dan melalui program pelatihan dan edukasi. Setelah kebijakan ini ditetapkan, pengendalian dapat diimplementasikan.

Pengendalian (Control)

Merupakan mekanisme yang diterapkan, baik untuk melindungi perusahaan dari risiko atau untuk meminimalkan dampak risiko tersebut pada perusahaan jika risiko tersebut terjadi.

Pengendalian terbagi menjadi tiga kategori, yakni:

1. Pengendalian Teknis
2. Pengendalian Formal
3. Pengendalian Informal

Pengendalian Teknis

Adalah pengendalian yang menjadi satu di dalam system dan dibuat oleh para penyususn system selama masa siklus penyusunan system.Dilakukan melalui tiga tahap:

1. Identifikasi Pengguna.
   Memberikan informasi yang mereka ketahui seperti kata sandi dan nomor telepon.nomor telepon.

2. Otentikasi Pengguna
   Pengguna memverivikasi hak akses dengan cara memberikan sesuatu yang mereka miliki, seperti chip identifikasi atau tanda tertentu.

3. Otorisasi Pengguna
   Pengguna dapat mendapatkan wewenang untuk memasuki tingkat penggunaan tertentu.
   Setelah pengguna memenuhi tiga tahap tersebut, mereka dapat menggunakan sumber daya informasi yang terdapat di dalam batasan file akses.

Sistem Deteksi Gangguan

Logika dasar dari sistem deteksi gangguan adalah mengenali upaya pelanggaran keamanan sebelum memiliki kesempatan untuk melakukan perusakan.
Contoh:
Peranti lunak proteksi virus (virus protection software).Peranti lunak yang didesain untuk mencegah rusaknya keamanan sebelum terjadi.

Firewall

Suatu Filter yang membatasi aliran data antara titik-titik pada suatu jaringan-biasanya antara jaringan internal perusahaan dan Internet.
Berfungsi sebagai:

1. Penyaring aliran data
2. Penghalang yang membatasi aliran data ke dan dari perusahaan tersebut dan internet.

Jenis:
Firewall Paket
Firewall Tingkat Sirkuit
Firewall Tingkat Aplikasi

Pengendalian Kriptografis

Merupakan penggunaan kode yang menggunakan proses-proses matematika.Meningkatkan keamanan data dengan cara menyamarkan data dalam bentuk yang tidak dapat dibaca. Berfungsi untuk melindungi data dan informasi yang tersimpan dan ditransmisikan, dari pengungkapan yang tidak terotorisasi.

- Enkripsi: merubah data asli menjadi data tersamar.
- Deksipsi: merubah data tersamar menjadi data asli.

Kriptografi terbagi menjadi:

1. Kriptografi Simetris
   Dalam kriptografi ini, kunci enkripsi sama dengan kunci dekripsi.

2. Kriptografi Asimetris

Dalam kriptografi ini, kunci enkripsi tidak sama dengan kunci dekripsi.
Contoh:
Enkripsi→ kunci public
Dekripsi→ Kunci Privat

3. Kriptografi Hybrid
Menggabungkan antara kriptografi simetris dan Asimetris, sehingga mendapatkan kelebihan dari dua metode tersebut.

Contoh:
SET (Secure Electronic Transactions) pada E-Commerce

Pengendalian Fisik

Peringatan yang pertama terhadap gangguan yang tidak terotorisasi adalah mengunci pintu ruangan computer.Perkembangan seterusnya menghasilkan kunci-kunci yang lebih canggih, yang dibuka dengan cetakan telapak tangan dan cetakan suara, serta kamera pengintai dan alat penjaga keamanan.

Pengendalian Formal

Pengendalian formal mencakup penentuan cara berperilaku,dokumentasi prosedur dan praktik yang diharapkan, dan pengawasan serta pencegahan perilaku yang berbeda dari panduan yang berlaku. Pengendalian ini bersifat formal karena manajemen menghabiskan banyak waktu untuk menyusunnya, mendokumentasikannya dalam bentuk tulisan, dan diharapkan untuk berlaku dalam jangka panjang.

Pengendalian Informal

Pengendalian informal mencakup program-program pelatihan dan edukasi serta program pembangunan manajemen.Pengendalian ini ditunjukan untuk menjaga agar para karyawan perusahaan memahami serta mendukung program keamanan tersebut.

Pentingnya Keamanan system

Sistem Informasi diperlukan karena:

1. Teknologi Komunikasi Modern yang membawa beragam dinamika dari dunia nyata ke dunia virtual
Contohnya adalah: dalam bentuk transaksi elektronik seperti e-banking, dan pembawa aspek positif maupun negative, misalnya: pencurian, pemalsuan, dan penggelapan menggunakan internet.

2. Kurangnya Keterampilan Pengamanan yang dimiliki oleh Pemakai
Contoh: Pemakai kurang menguasai computer.

3. Untuk menjaga objek kepemilikan dari informasi yang memiliki nilai ekonomis.
Contoh: dokumen rancangan produk baru, kartu kredit, dan laporan keuangan perusahaan

Dukungan Pemerintah Dan Industri

Beberapa organisasi pemerintah dan internasional telah menentukan standar-standar yang ditunjukan untuk menjadi panduan bagi organisasi yang ingin mendapatkan keamanan informasi.Beberapa standar ini berbentuk tolak ukur, yang telah diidentifikasisebelumnya sebagai penyedia strategi alternative untuk manajemen resiko. Beberapa pihak penentu standar menggunakan istilah baseline(dasar) dan bukannya *benchmark* (tolak ukur). Organisasi tidak diwajibkan mengikuti standar ini.Namun, standar ini ditunjukan untuk memberikan bantuan kepada perusahaan dalam menentukan tingkat target keamanan.

Manajemen Keberlangsungan Bisnis

Manajemen keberlangsungan bisnis (business continuity management-BCM) adalah aktivitas yang ditujukan untuk menentukan operasional setelah terjadi gangguan sistem informasi.

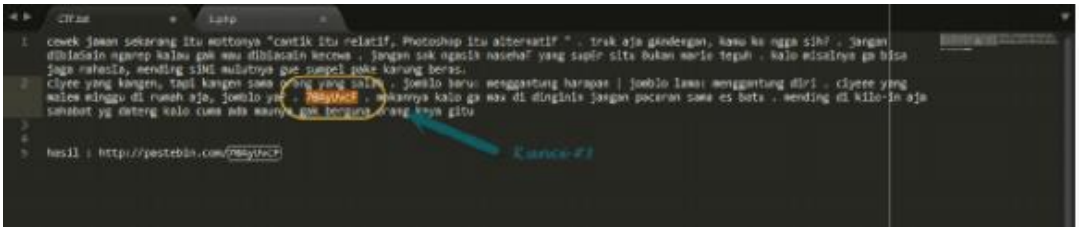
Subrencana yang umum mencakup:

- Rencana darurat (emergency plan): terdiri dari cara-cara yang akan menjaga keamanan karyawan jika bencana terjadi. Co: Alarm bencana, prosedur evakuasi
- Rencana cadangan : menyediakan fasilitas computer cadangan yang bisa dipergunakan apabila fasilitas computer yang biasa hancur atau rusak hingga tidak bisa digunakan.
- Rencana catatan penting (vital records plan) : merupakan dokumen kertas, microform, dan media penyimpanan optis dan magnetis yang penting untuk meneruskan bisnis perusahaan.

Jawaban no.2

Pada kasus ini, penulis akan memberikan contoh pengungkapan bukti informasi yang terkandung dalam sebuah file text dengan ekstensi .txt. Dalam kasus ini, penulis mengambil contoh penyelesaian Soal Cyber Jawara Competition 2014. Berikut ini screen shoot hasil investigasi yang dilakukan :

1. Dalam soal terdapat sebuah file ctf.txt, setelah dilakukan analisa tentang properties dan string yang terkandung di dalamnya, tidak ditemukan sesuatu yang mencurigakan yang harus di eksplor lebih jauh. Akhirnya analisa dilanjutkan untuk membuka isi file dan mencernanya. Ditemukan rangkaian typografi dalam file ctf.txt, dimana merujuk ke url http://pastebin.com/70AyUvcF

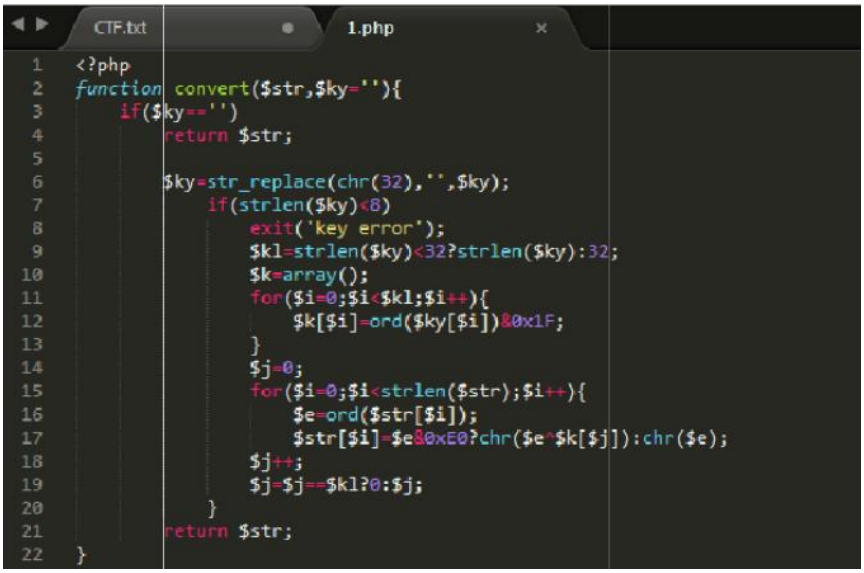


2. Setelah diakses situs tersebut, ditemukan kode PHP seperti dibawah ini :

```
function convert($str,$ky=''){
if($ky=='')return $str;
$ky=str_replace(chr(32),'',$ky);
if(strlen($ky)<8)exit('key error');
$kl=strlen($ky)<32?strlen($ky):32;
$k=array();for($i=0;$i<$kl;$i++){
$k[$i]=ord($ky[$i])&0x1F;}
$j=0;for($i=0;$i<strlen($str);$i++){
$e=ord($str[$i]);
$str[$i]=$e&0xE0?chr($e^$k[$j]):chr($e);
$j++;$j=$j==$kl?0:$j;}
return $str;
}

$key='Nama Web';
$string1='';
```

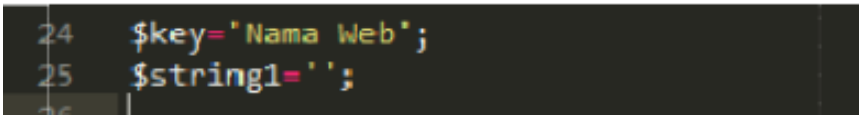
3. Kemudian dilakukan perbaikan pada kode tersebut dan memasukkan beberapa slue enkrip yang terdapat pada file ctf.txt seperti di bawah ini :



```
<?php
function convert($str,$ky=''){
    if($ky=='')
        return $str;

    $ky=str_replace(chr(32),'',$ky);
        if(strlen($ky)<8)
            exit('key error');
            $kl=strlen($ky)<32?strlen($ky):32;
            $k=array();
            for($i=0;$i<$kl;$i++){
                $k[$i]=ord($ky[$i])&0x1F;
            }
            $j=0;
            for($i=0;$i<strlen($str);$i++){
                $e=ord($str[$i]);
                $str[$i]=$e&0xE0?chr($e^$k[$j]):chr($e);
            $j++;
            $j=$j==$kl?0:$j;
        }
    return $str;
}
```

4. Setelah melakukan berbagai percobaan, disimpulkan bahwa dua clue string pada script PHP harus diperlakukan berbeda



```
$key='Nama Web';
$string1='';
```

5. Dan setelah dibuka file pastebin dari pengupload file diperoleh kemudian kami disini harus bisa mendapatkan isi kedua variabel berikut :

Dan isinya :

Isinya : V mrs%8)Z$ifKB1cl U

6. Setelah dimasukkan pada script PHP $string1 = V mrs%8)Z$ifKB1cl U
   Menghasilkan kode seperti dibawah ini :

```php
<?php
function convert($str,$ky=''){
    if($ky=='')
        return $str;

    $ky=str_replace(chr(32),'',$ky);
        if(strlen($ky)<8)
            exit('key error');
        $kl=strlen($ky)<32?strlen($ky):32;
        $k=array();
        for($i=0;$i<$kl;$i++){
            $k[$i]=ord($ky[$i])&0x1F;
        }
        $j=0;
        for($i=0;$i<strlen($str);$i++){
            $e=ord($str[$i]);
            $str[$i]=$e&0xE0?chr($e^$k[$j]):chr($e);
        $j++;
        $j=$j==$kl?0:$j;
        }
    return $str;
}

$key='pastebin';
$string1='Vmrs%8)Z$ifKB1c| U';

echo convert($string1,$key);

?>
```

7. Maka hasil yang akan ditampilkan pada localhots web server mesin adalah T4hu_G3jr0T

KESIMPULAN

Forensik adalah sebuah metode untuk mendapatkan bukti-bukti baru guna mengungkapkan sebuah kasus, khususnya kasus kejahatan. Kata kunci yang dapat digunakan untuk forensik adalah penelusuran, investigasi yang dilakukan secara sistematis dan ilmiah. Pada contoh digital forensik yang telah dijelaskan di atas, terkadang dalam memperoleh bukti baru sebuah bukti digital, diperlukan teknik ilmiah dan kecerdasan dalam berpikir. Clue T4hu_G3jr0T pada hasil akhir menunjukan sebuah key atau kunci yang mungkin digunakan sebagai password atau login ke sebuah akun atau untuk membongkar sebuah file rar yang terproteksi. Artinya, metode forensik sangatlah penting dalam membantu proses penyelidikan guna menghasilkan alat bukti yang sah, kuat dan dapat dipertanggungjawabkan secara hukum di depan pengadilan