UAS

(*Ujian Akhir Semester*)

Keamanan Informasi

Oleh

Nama : Gede Doni Ariawan

Nim : 1310651069

Kelas : A

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2014/2015

Soal :

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Jawaban :

Business Continuity and Disaster Recovery Planning

Business Continuity Plan (BCP) adalah rencana yang fokus untuk mempertahankan kelangsungan fungsi bisnis saat gangguan terjadi dan sesudahnya sehingga dapat meminimalisasi kerugian yang diakibatkan oleh bencana. Secara sederhana, perencanaan kelangsungan bisnis (Bahasa Inggris: business continuity planning, BCP) atau sebutan lainnya adalah disaster and recovery planning atau DRP), diciptakan untuk mencegah gangguan terhadap aktivitas bisnis normal. BCP dirancang untuk melindungi proses bisnis yang kritis dari kegagalan akibat dari bencana, yang dapat mengakibatkan hilangnya kemampuan perusahaan dalam melakukan proses bisnis secara normal. BCP merupakan suatu strategi untuk memperkecil efek gangguan dan untuk memungkinkan proses bisnis terus berlangsung.
Bencana Bencana yang dimaksud dalam BCP ini adalah semua peristiwa yang terjadi dan mempunyai potensi mengganggu jalannya proses usaha dalam keadaan normal (BAU - Business As Usually).

Disaster Recovery Planning (DRP) adalah rencana yang fokus pada sistem teknologi informasi yang diterapkan pada data center untuk memperbaiki operabilitas sistem target, aplikasi, dan fasilitas komputer dilokasi alternatif dalam kondisi darurat. Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. Pengertian ini mengidentifikasikan sebuah

kejadian yang tiba-tiba, tidak diharapkan, bersifat sangat merusak, dan kurang perencanaan. Bencana terjadi dengan frekuensi yang tidak menentu dan akibat yang ditimbulkannya meningkat bagi mereka yang tidak mempersiapkan diri terhadap kemungkinan-kemungkinan timbulnya bencana.

Berbagai bencana yang mungkin terjadi antara lain adalah Kebakaran, banjir, gempa bumi,angin topan konsleting listrik, Serangan terorisme, Sistem atau perangkat yang rusak, Kesalahan operasional akibat ulah manusia, Virus dan lain-lain.

Bisnis akan bergantung pada informasi yang tersebar dan aplikasi yang memproses informasi tersebut, sehingga aplikasi penopang utama yang spesifik menjadi sangat kritikal sehingga ketika terjadi gangguan hanya beberapa saat maka dapat melumpuhkan kelangsungan bisnis perusahaan. Oleh karenanya, beberapa perusahaan mempunyai suatu arahan yang menjamin availabilitas kelangsungan bisnis ketika terjadi suatu bencana/gangguan yang tidak direncanakan atau sudah direncanakan.

Tujuan BCP adalah untuk memperkecil efek peristiwa mengganggu tersebut pada operasional perusahaan dan mengurangi risiko kerugian keuangan dan meningkatkan kemampuan organisasi dalam proses pemulihan sesegera mungkin dari suatu peristiwa yang mengganggu. BCP juga membantu memperkecil biaya yang berhubungan dengan peristiwa yang mengganggu tersebut dan mengurangi risiko yang berhubungan dengan itu.

Business Continuity Plan perlu melihat pada semua area pengolahan informasi kritis perusahaan. Proses adalah proses bisnis yang berjalan pada lokasi perusahaan. Proses usaha ini harus di identifikasi agar proses yang inti/utama dapat dilakukan pada tempat usaha/lokasi yang lain agar apabila pada lokasi usaha tersebut terdapat ganguan maka proses tetap dapat berjalan dari tempat/lokasi BCP.

Lokasi/Place Lokasi atau tempat merupakan tempat yang letaknya bukan di lokasi/tempat yang sama dengan tempat bisnis dilakukan dan pada lokasi/tempat ini dapat digunakan untuk melakukan kegiatan bisnis/tempat kerja/workspase. Tempat untuk menyimpan arsip dan lain lain Untuk mencari tempat yang baik diperlukan Risk

Assessment.

Teknologi/IT Teknologi merupakan alat/tools yang digunakan oleh binis untuk menjalankan bisnisnya termasuk infrastruktur (Network, Komunikasi, Jaringan dll).

Tahapan pembentukan BCP/DRP untuk membuat sebuah BCP/DRP memiliki beberapa tahapan yang harus dilakukan sebagai berikut

1. Penilaian resiko (Risk Assessment)
2. Analisa dampak bisnis (Bisnis Impact Analysis)
3. Perencanaan BCP (Planning)
4. Pembentukan BCP (Developing)
5. Test, pemeliharaan dan audit BCP (Testing, Maintaining and Auditing)

Model lainnya dalam pembuatan BCP/DRP mengukip dari ISO22301:2012 adalah PDCA

1. Establish (PLAN)
2. Implement and Operate (Do)
3. Monitor and Review (Check)
4. Maintain and Improve (Act)

BCP/DRP Dokumen harus dilakukan review secara berkala beberapa hal yang mengharuskan BCP/DRP diperbaiki adalah

- Adanya perubahan yang signifikan pada struktur organisasi
- Adanya perubahan yang signifikan pada system

apabila tidak dilakukan perubahan dengan segera maka BCP/DRP dokumen yang kita miliki tersebut dapat dikatakan TIDAK SESUAI/ TIDAK DAPAT dipergunakan lagi.

Soal :

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

Jawaban :

Mengunci file atau data yang ada pada suatu folder dengan menggunakan software secure folder dan menangani kasus penyalahgunaan Data atau informasi pada PC.

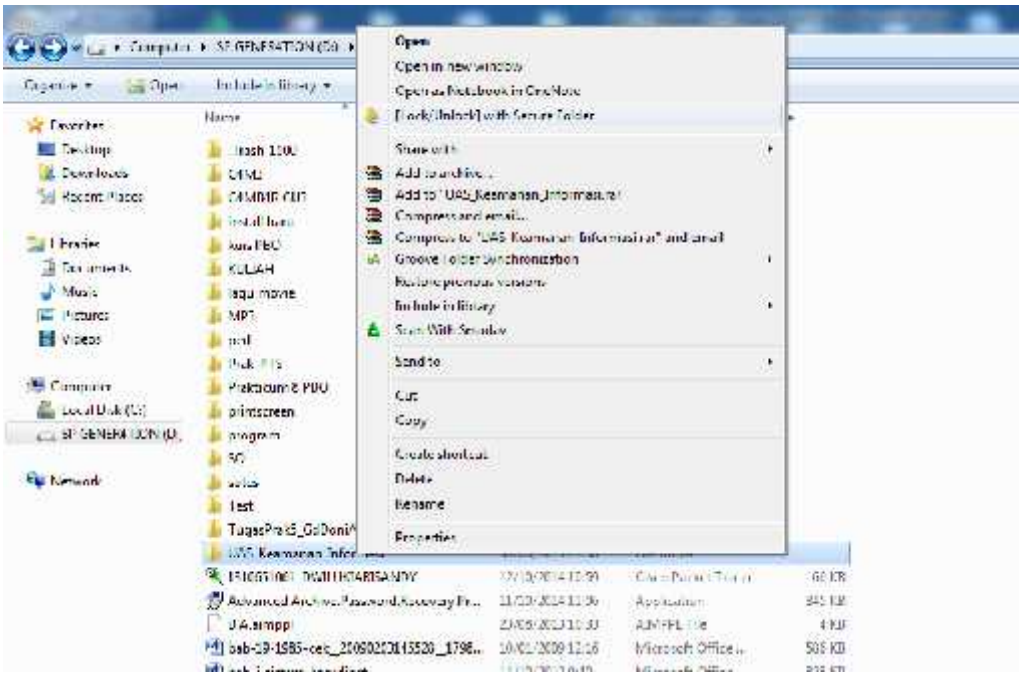
Untuk menyembunyikan file dan informasi penting biasanya kita menyimpannya dalam folder khusus agar tidak ada seorangpun yang bisa menemukannya. Teknik hidden file mudah dijebol karena sudah banyak orang yang tahu sehingga file atau informasi yang ada pada PC kita mudah untuk dibuka atau disalahgunakan,
Menurut saya cara memproteksi file atau informasi yang ada pada folder yang paling aman adalah dengan memberi password pada folder tersebut. Sebenarnya di windows sendiri sudah ada setingan untuk memproteksi folder, tapi menurut saya cara tersebut kalo orang jawa bilang “njilmet”.
Maka dari itu kali ini kita akan membahas cara mengunci folder dengan sotware mungil tapi ampuh. Software untuk mengunci folder yang akan kita gunakan adalah secure folder. Software ini berukuran sangat kecil hanya sekitar 1,3 MB untuk yang versi standar dan versi portable 430 kb saja. Meskipun berukuran kecil software ini mampu memproteksi folder anda dengan password yang bisa anda tentukan sendiri.

Berikut saya jelaskan cara Mengunci Folder yang berisi file dan informasi Dengan Secure Folder :

1. Silahkan download dulu aplikasinya,
2. Untuk cara penggunaanya sendiri terbilang cukup mudah :
   Install secure folder
   Setelah selesai anda akan diminta untuk membuat sebuah password. Isi kolom password dan email jika suatu saat anda lupa passwordnya anda bisa mendapatkan password baru menggunakan email anda.
   confirm password lalu klik set.

Password tersebut nantinya akan digunakan untuk membuka folder yang anda kunci.

Untuk mengunci folder langkah-langkahnya adalah sebagai berikut. Klik kanan pada folder yang ingin anda proteksi dengan password. Lalu pilih [lock/unlock] with secure folder.



Kemudian pilih lock.

Dan folder tersebut akan terkunci dan tidak bisa dibuka kembali.

Jika ingin membukanya, caranya sama dengan menguncinya yaitu klik kanan pada folder . Lalu pilih [lock/unlock] with secure folder. masukan password dan folder bisa dibuka kembali.