UJIAN AKHIR SEMESTER

MATA KULIAH ETIKA PROFESI

JURUSAN SISTEM INFORMASI

UNIVERSITAS SRIWIJAYA

Nama : Zhafira Zafitri
NIM : 09031382025125
Kelas : SI BIL 5B

Petunjuk:

Kerjakan soal berikut secara mandiri

Jawablah soal sesuai dengan pertanyaannya

Jangan lupa tuliskan nama,NIM dan kelas saudara pada lembar jawaban

Soal:

1. Jelaskan dua macam ancaman terhadap system informasi!

   Jawab :

   a) Ancaman aktif merupakan suatu kejahatan yang terjadi pada komputer dan suatu kecurangan berupa pencurian data. Ancaman aktif mencakup :
      - Pencurian data.
        Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau uang. Misalnya, mata-mata industri dapat memperoleh informasi persaingan yang berharga, penjahat komputer dapat mencuri uang bank.
      - Penggunaan sistem secara ilegal.
        Orang yang tidak berhak mengakses informasi pada suatu sistem yang bukan menjadi hak-nya, dapat mengakses sistem tersebut. Penjahat komputer jenis ini umumnya adalah hacker yaitu orang yang suka menembus sistem keamanan dengan tujuan mendapatkan data atau informasi penting yang diperlukan, memperoleh akses ke sistem telepon, dan membuat sambungan telepon jarak jauh secara tidak sah.
      - Penghancuran data secara ilegal.
        Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu sistem operasi komputer. Penjahat komputer ini tidak perlu berada ditempat kejadian. Ia dapat masuk melalui jaringan komputer dari suatu terminal dan menyebabkan kerusakan pada semua sistem dan hilangnya data atau informasi penting. Penjahat komputer jenis ini umumnya disebut sebagai cracker yaitu penjebol sistem komputer yang

bertujuan melakukan pencurian data atau merusak sistem.

- Modifikasi secara ilegal Perubahan-perubahan pada data atau informasi dan perangkat lunak secara tidak disadari.
  Jenis modifikasi yang membuat pemilik sistem menjadi bingung karena adanya perubahan pada data dan perangkat lunak disebabkan oleh progam aplikasi yang merusak (malicious software). Program aplikasi yang dapat merusak tersebut terdiri dari program lengkap atau segemen kode yang melaksanakan fungsi yang tidak dikehendaki oleh pemilik sistem. Fungsi ini dapat menghapus file atau menyebabkan sistem terhenti. Jenis aplikasi yang dapat merusak data atau perangkat lunak yang paling populer adalah virus.

b) Ancaman pasif merupakan kegagalam sistem itu sendiri atau kesalahan manusia dalam memproses sistem, atau karena adanya bencana alam yang terjadi yang mengakibatkan ancaman bagi sistem itu sendiri.

- Kegagalan sistem.
  Kegagalan sistem atau kegagalan software dan hardware dapat menyebabkan data tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. Selain itu, tegangan listrik yang tidak stabil dapat membuat peralatan-peralatan menjadi rusak dan terbakar.
- Kesalahan manusia.
  Kesalahan pengoperasian sistem yang dilakukan oleh manusia dapat mengancam integritas sistem dan data.
- Bencana alam.
  Bencana alam seperti gempa bumi, banjir, kebakaran, hujan badai merupakan faktor yang tidak terduga yang dapat mengancam sistem informasi sehingga mengakibatkan sumber daya pendukung sistem informasi menjadi luluhlantah dalam waktu yang singkat.

2. Sebutkan enam metode yang umum digunakan untuk masuk kedalam system berbasis computer!

   Jawab :

   Metode yang umum digunakan oleh orang untuk masuk kedalam sistem berbasis komputer ada 6 macam yaitu:

   1. Pemanipulasian masukan.
   2. Penggantian program.
   3. Penggantian secara langsung.
   4. Pencurian data.
   5. Sabotase.
   6. Penyalahgunaan dan pencurian sumber daya komputasi.

3. Sebutkan dan jelaskan empat rencana pengamanan system informasi terhadap bencana!

   Jawab :

1. Disaster Recovery Jaringan

   Disaster recovery ini berpusat pada pemulihan jaringan. Metode ini berkembang dari

asumsi bahwa jaringan suatu perusahaan merupakan aspek penting yang harus turut diselamatkan saat bencana melanda. Prosedur pemulihan jaringan umumnya melibatkan koneksi dengan anggota tim IT, penggantian perangkat jaringan, serta sejumlah usaha terkaitlain untuk memulihkan konektivitas yang sempat terputus.

2. Disaster Recovery Virtual

   Seperti namanya, *recovery* jenis ini mengandalkan metode virtualisasi dalam proses pemulihan data. Pusat data virtual ditempatkan untuk menggantikan *server* fisik sebagai perangkat utama. Tak jarang, metode ini juga didukung oleh sejumlah portal virtualisasi yangmenghadirkan layanan *backup* dan *restore*. Ketika terjadi bencana atau kerusakan, sistem pemulihan virtual akan segera melakukan tindakan penyelamatan data tanpa menunggu *server* fisik menyelesaikan beban kerjanya. Oleh karena itu, jenis *recovery* ini dianggap lebih menguntungkan dari segi efisiensi waktu.

3. Disaster Recovery dalam Pusat Data

   Pemulihan yang berpusat pada *data center* atau pusat data perusahaan ditempatkan dalam sebuah sistem khusus yang menggunakan fasilitas komputerisasi. Untuk bisa melakukan proses manajemen bencana, pusat data tersebut harus dikembangkan terlebih dahulu. Prosedur pengembangannya meliputi pengamanan lokasi, pemantapan perangkat dan pegawai, serta pengaturan HVAC ruangan (*heating, ventilation*, dan *air conditioning*). *Disaster recovery* pusat data dianggap sebagai solusi paling aman dan efektif bagi sebagian besar perusahaan. Namun, waktu pengembangan yang cukup panjang serta banyaknya unsurpenting yang harus dilibatkan membuat jenis manajemen bencana ini sering dirasa kurang praktis.

4. Disaster Recovery Berbasis Cloud

   Manajemen bencana berbasis *cloud*. Proses intinya berpusat pada *cloud storage*, yakni portalpenyimpanan dan pemulihan data yang diatur oleh penyedia layanan pihak ketiga.

   Dengan menggunakan *cloud-based disaster recovery*, perusahaan akan memiliki pusat data aman di dalam *cloud* tanpa perlu mengembangkan fasilitas sendiri atau mempekerjakantenaga ahli. Seluruh prosedur pengamanan data pun dijalankan secara lebih praktis. Salah satu contoh dari jenis *disaster recovery* ini adalah Azure Site Recovery. Denganmenggunakan pusat data berbasis *cloud services*, layanan tersebut akan membantu Anda memulihkan data saat terjadi bencana. Prosedur perlindungan dan pemulihan data yang dijalankan juga didukung oleh infrastruktur yang lengkap serta

layanan yang terintegrasi luas.