PEMBAHASAN UTS KJI 2018/2019

1. Jelaskan disertai contoh konsep CIA triad dalam keamanan informasi!
2. Jelaskan 6 unsur yang bertanggung jawab program keamanan informasi, serta perannya!
3. Jelaskan mengapa "pekerjaan yang dilakukan oleh pihak ketiga" merupakan salah satu rangkaian konsep dasar dari prosedur keamanan sistem informasi!
4. Jelaskan 3 alasan yang menyebabkan masih digunakannya sistem operasi lama dalam sistem perusahaan!
5. Jelaskan bagaimanakah peran physical security dalam membantu memberikan pengamanan informasi perusahaan! Berikan contoh satu kasus!

Jawab

1. – Confidentiality

   Pengertian : artinya kerahasiaan. Kerahasian dalam hal ini adalah informasi yang kita miliki pada sistem/database kita, adalah hal yang rahasia dan pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya

   Contoh Konsep : menerapkan enkripsi. Enkripsi merupakan sebuah teknik untuk mengubah file/data/informasi dari bentuk yang dapat dimengerti (plaintext) menjadi bentuk yang tidak dapat dimengerti (ciphertext), sehingga membuat attacker sulit untuk mendapatkan informasi yang mereka butuhkan.

   – Integrity

   Pengertian : Integrity maksudnya adalah data tidak dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, akurasi, dan validitas data tersebut masih terjaga.

   Contoh Konsep : rusaknya integrity terkait keamanan informasi adalah pada proses pengiriman email.

   – Availability

   Pengertian : memastikan sumber daya yang ada siap diakses kapanpun oleh user/application/sistem yang membutuhkannya.

   Contoh Konsep : steam, platform distribusi game digital terbesar di dunia, tidak bisa diakses atau mengalami server down oleh serangan Distributed Denial of Service (DDoS). Padahal pada waktu tersebut steam sedang dibanjiri pengunjung karena sedang mengadakan winter sale.

2. Yaitu :
   - **Senior Management** : Memastikan bahwa rekomendasi audit yang berkaitan dengan perlindungan informasi ditangani secara tepat waktu dan memadai.
   - **Information Security management** : Mendorong upaya untuk membuat, menerbitkan, dan menerapkan kebijakan dan standar keamanan informasi
   - **Business Unit Managers** : Memastikan sumber daya tersedia untuk menyusun, menguji, dan memelihara rencana bisnis kesinambungan di bawah koordinasi manajer Keamanan Informasi atau yang ditunjuk oleh manajer IS.
   - **First Line Supervisors** : Memantau aktivitas pekerja mereka sehubungan dengan kebijakan dan standar keamanan informasi organisasi

- **Employees** : program keamanan informasi hanya berfungsi dengan baik jika semua pekerja berpartisipasi, dan pekerja berpartisipasi dengan sukarela karena mereka merasa mereka memiliki peran nyata untuk dilakukan.
- **Third Parties** : Bertanggung jawab mematuhi kebijakan dan standar keamanan informasi dari pihak organisasi yang berkontrak atau pihak mereka berikan layanan.

3. Karena harus bertanggung jawab mematuhi kebijakan dan standar keamanan informasi dari pihak organisasi yang berkontrak atau pihak mereka berikan layanan. Hal ini secara jelas harus dinyatakan dalam kontrak apa pun yang mengikat kedua pihak.

4. Yaitu :
   - Sudah cukup puas dengan aplikasi yang ada
   - Tidak tersedianya biaya yang cukup untuk pengembangan
   - SDM yang kurang tanggap dengan laju teknologi, dsb.

5. Physical security adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam. Contohnya apabila PC yang memiliki resiko tinggi dan bersifat *stand alone*, akan lebih baik apabila *physical security* juga diterapkan misalnya meletakkan PC terkait di ruangan khusus / sendiri yang hanya dapat diakses oleh orang-orang tertentu sehingga dapat dikontrol penggunanya.