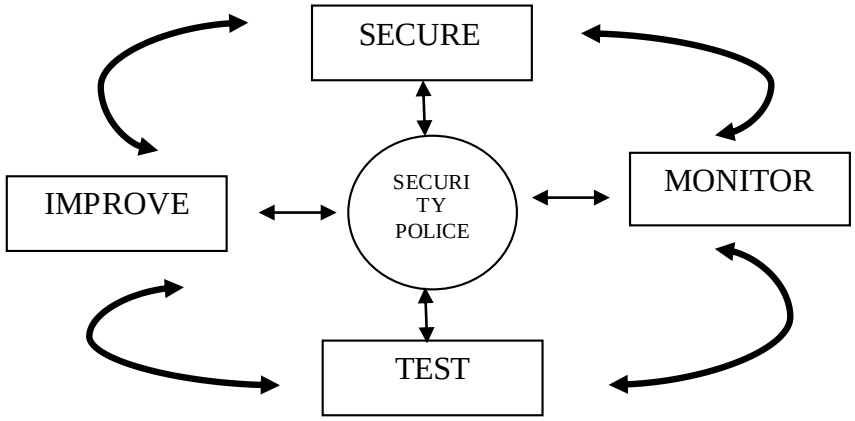
PEMBAHASAN SOAL UTS KJI 2019/2020

1. Security Wheel menurut Peltier



Menurut Peltier, kebijakan keamanan ada 4 yaitu Secure (Aman), Improve (Memperbaiki), Test (Menguji), Monitor (Memonitor). Keempat hal tersebut saling berkaitan dan memiliki peran masing-masing dalam kebijakan keamanan.
Secure adalah tahap mengamankan jaringan dengan menerapkan solusi keamanan misalnya penyaringan paket dan pertahanan ancaman. Selanjutnya ada tahap Monitor yaitu tahap dimana proses pemantauan keamanan melibatkan metode aktif dan pasif dalam memonitor pelanggaran keamanan. Setelah dilakukan monitor maka akan dilakukan test yaitu tahap pengujian keamanan setelah dilakukan beberapa hal terkait kebijakan keamanan. Terakhir adalah Improve, yaitu tahap yang dilakukan setelah melakukan test, dilihat apakan ada hal yang perlu diperbaiki dari kebijakan keamanan yang telah dilakukan untuk keamanan yang lebih baik lagi.
Tahap-tahap tersebut akan dilakukan lagi dan lagi guna mendapatkan keamanan yang maksimal terutama pada tahap improve.

2. Contoh kasus: Bocornya data pada perusahaan pelayanan cloud dan keamanan.
   Unsur-unsur yang bertanggung jawab pada program keamanan informasi
   a. Senior manajement
      Memastikan bahwa rekomendasi audit yang berkaitan dengan
      perlindungan informasi ditangani secara tepat waktu dan memadai dan memberikan resolusi untuk masalah yang ada untuk diatasu berdasarkan basis organisasi.
   b. Information Security Management
      Membuat, menerbitkan, dan menerapkan kebijakan dan standar keamanan informasi dan mengelola upaya keamanan informasi di dalam unit keamanan informasi.
   c. Business Unit Managers
      Melakukan peninjauan kebijakan, mengukur keamanan informasi di dalam unit, dan memastikan sumber daya tersedia untuk menyusun, menguji dan memelihara rencana bisnis berkesinambungan.
   d. First Line Supervisors

Mengkomunikasikan masalah keamanan kepada Keamanan Informasi dan Senior Manajement.

e. Employees
   Melakukan kebijakan keamanan yang telah sepakati perusahaan.
f. Third Parties
   Bertanggung jawab mematuhi kebijakan dan standar keamanan informasi dari pihak organisaisi yang berkontrak.

3. Arti CIA Triad dan masing-masing contoh kasusnya
   CIA Triad adalah suatu model yang dirancang atau didesain dengan tujuan memandu kebijakan yang terkait dengan keamanan informasi pada suatu organisasi. Reputasi organisasi akan dipandang baik bagi khalayak umum apabila dapat diyakinkan oleh 3 hal, yaitu Confidentiality, Integrity, dan Availability.
   a. Confidentiality (Kerahasiaan)
      Kerahasiaan informasi yang kita miliki pada sistem/ database adalah hal yang rahasia dan pengguna atau orang yang tidak berkepentingan tidak dapat melihat/ mengaksesnya.
      Contoh: Database suatu perusahaan hanya dapat diakses oleh orang yang mempunyai wewenang atau berkepentingan dalam database tersebut. Tidak sembarangan orang bisa mengakses suatu database perusahaan sekalipun dia sebagai pegawai di perusahaan tersebut karena semakin banyak orang yang bisa mengaskes database tersebut maka kemungkinan kebocoran akses database menjadi besar. Database perusahaan yang sifatnya sangat rahasia akan bisa dimanipulasi atau diambil datanya oleh orang yang tidak bertanggung jawab.
   b. Integrity
      Integrity adalah data tidak dapat diubah dari aslinya oleh orang yang tidak berhak, sehingga konsisten, akurat, dan validitas data tersebut bisa terjaga.
      Contoh: Data penting milik perusahaan tidak boleh diubah oleh sembarang orang karena perusahaan akan kehilangan data asli dan mereka tidak mengetahui apa yang diubah dari data tersebut.
   c. Availability
      Memastikan sumber daya yang ada siap diakses kapanpun oleh user/ application/ system yang membutuhkan.
      Contoh: Pada SIAP atau Kulon2, jika sedang diadakan kuis untuk seluruh mahasiswa semester 4 dan terjadi down atau tidak bisa diakses, maka itu sangat menganggu dan mengurangi kenyamanan user dalam mengakses SIAP atau Kulon2 saat melakukan hal penting seperti mengakses kuis tersebut.