JAWABAN HANYA REFERENSI DAN BELUM TENTU BENAR

PEMBAHASAN UTS KEAMANAN DAN JAMINAN INFORMASI

SEMESTER GASAL TAHUN AJARAN 2022/2023

1. Jelaskan gambaran umum mengenai security wheel dan hubungannya dengan CIA Triad pada keamanan informasi!
   Jawab :

CIA Triad

Security wheel adalah suatu konsep atau model yang membantu menggambarkan dan mengelola keamanan informasi secara menyeluruh. Konsep ini menggambarkan pendekatan yang holistik terhadap keamanan informasi dengan mempertimbangkan berbagai aspek keamanan, termasuk ketersediaan (*availability*), integritas (*integrity*), kerahasiaan (*confidentiality*), otentikasi (*authentication*), otorisasi (*authorization*), dan *non-repudiation*. Sementara itu, CIA Triad adalah konsep dasar dalam keamanan informasi yang terdiri dari tiga komponen utama:

a. Kerahasiaan (*Confidentiality*): Menunjukkan bahwa informasi hanya dapat diakses oleh orang yang memiliki hak untuk mengaksesnya dan harus dijaga dari akses yang tidak sah.
b. Integritas (*Integrity*): Menekankan bahwa informasi harus tetap utuh, tidak diubah secara tidak sah, dan hanya dapat diubah oleh orang yang memiliki otoritas untuk melakukannya.
c. Ketersediaan (*Availability*): Menggambarkan bahwa informasi harus tersedia dan dapat diakses oleh orang yang memiliki hak untuk mengaksesnya pada saat dibutuhkan.

Hubungan antara *security wheel* dan CIA Triad terletak pada integrasi prinsip-prinsip CIA Triad ke dalam konsep *security wheel*. *Security wheel* melengkapi dan memperluas konsep CIA Triad dengan mempertimbangkan aspek lain dari keamanan informasi, seperti otentikasi, otorisasi, dan non-repudiation. Dalam implementasi keamanan informasi yang efektif, kedua konsep ini harus diintegrasikan untuk memastikan keamanan yang komprehensif, baik dari segi konfidensialitas, integritas, maupun ketersediaan informasi.

JAWABAN HANYA REFERENSI DAN BELUM TENTU BENAR

2. Sebutkan dan jelaskan tiga unsur penanggung jawab keamanan informasi beserta perannya!
   Jawab :
   a. Senior Management, berperan :
      - Memastikan bahwa rekomendasi audit yang berkaitan dengan perlindungan informasi ditangani secara tepat waktu dan memadai
      - Berpartisipasi dalam kegiatan Komite Pengarah Keamanan Informasi untuk memandu kegiatan upaya keamanan informasi
      - Mengawasi pembentukan, pengelolaan, dan kinerja dari unit keamanan informasi (termasuk menyediakan sumber dayanya)
      - Berpartisipasi dalam upaya untuk mendidik staf organisasi tentang tanggung jawab mereka untuk melindungi informasi
      - Meninjau dan menyetujui kebijakan dan strategi keamanan informasi
      - Memberikan resolusi untuk masalah keamanan informasi yang besar atau urgent untuk diatasi berdasarkan basis organisasi.
   b. Information Security Management, berperan :
      - Mendorong upaya untuk membuat, menerbitkan, dan menerapkan kebijakan dan standar keamanan informasi
      - Mengkoordinasikan pembuatan dan pengujian rencana bisnis kesinambungan
      - Mengelola upaya keamanan informasi di dalam unit keamanan informasi
      - Mengelola perangkat lunak keamanan informasi atas nama organisasi
      - Memberikan program pendidikan dan kesadaran yang cukup untuk organisasi.
   c. Business Unit Managers, berperan :
      - Berpartisipasi dalam proses peninjauan kebijakan
      - Memberi masukan untuk standar keamanan informasi
      - Mengukur keamanan informasi di dalam unit
      - Menegakkan kepatuhan dengan kebijakan dan standar
      - Mendukung pendidikan dan kesadaran keamanan informasi\
      - Memastikan sumber daya tersedia untuk menyusun, menguji, dan memelihara rencana bisnis kesinambungan di bawah koordinasi manajer Keamanan Informasi atau yang ditunjuk oleh manajer IS.
3. Mengapa kebijakan merupakan salah satu unsur penting dalam keamanan informasi? Jelaskan peran kebijakan sebagai unsur penting dalam keamanan informasi!
   Jawab :
   Kebijakan menjalankan dua peran yaitu peran internal dan peran eksternal.
   a. Bagian internal memberi tahu karyawan apa yang diharapkan dari mereka dan bagaimana tindakan mereka akan dinilai.

JAWABAN HANYA REFERENSI DAN BELUM TENTU BENAR

b. Bagian eksternal memberi tahu dunia bagaimana perusahaan dijalankan, bahwa ada kebijakan yang mendukung praktik bisnis yang sehat, dan bahwa organisasi memahami bahwa perlindungan aset sangat penting untuk keberhasilan pelaksanaan misinya.

4. Salah satu upaya perlindungan fisik terhadap keamanan informasi adalah dengan mengimplementasikan sistem deteksi intrusi. Apakah tujuan dari sistem tersebut? Serta jelaskan elemen yang digunakan dalam sistem tersebut!
   Jawab :

   Tujuan dari sistem deteksi intrusi adalah untuk mendeteksi serangan keamanan atau pelanggaran kebijakan keamanan, memberikan tindakan respons cepat, dan membantu melindungi integritas, kerahasiaan, dan ketersediaan sistem dan data. Elemen –elemen utama yang digunakan dalam sistem deteksi intrusi adalah sebagai berikut :

   a. Sensor atau Sensor Agent:
      komponen yang bertanggung jawab untuk memonitor lalu lintas jaringan atau aktivitas sistem. Sensor ini mengumpulkan data yang diperlukan untuk menganalisis dan mendeteksi potensi aktivitas mencurigakan atau ancaman keamanan.
   b. Analyzer (Analisis Engine):
      menganalisis data yang dikumpulkan oleh sensor untuk mengidentifikasi pola atau tanda-tanda serangan atau perilaku yang mencurigakan. Analisis ini dapat menggunakan aturan, algoritma, atau metode kecerdasan buatan untuk mendeteksi serangan.
   c. Database Penanda (Signature Database):
      berisi pola atau tanda-tanda serangan yang telah diketahui sebelumnya. Sistem deteksi intrusi membandingkan aktivitas yang diamati dengan tanda-tanda dalam database penanda untuk mendeteksi serangan yang telah dikenal.
   d. Manajemen Kejadian dan Respon (Event Management and Response):
      bertanggung jawab untuk mengelola peristiwa yang terdeteksi, memberikan peringatan atau tindakan respons sesuai dengan kebijakan yang telah ditentukan, dan melacak kejadian untuk analisis lebih lanjut dan perbaikan keamanan.

5. Dalam analisis dan manajemen risiko terkait keamanan informasi, mengidentifikasi risiko merupakan langkah awal yang penting. Namun mengetahui risiko yang akan dihadapi saja tidaklah cukup. Terdapat hal-hal yang bias dilakukan dalam mengurangi risiko yang sudah diidentifikasi. Jelaskan strategi yang dapat digunakan dalam mengurangi risiko keamanan informasi dan berikan masing masing contohnya!
   Jawab :
   Terdapat empat strategi berbeda untuk mengurangi resiko, yaitu :
   - Avoid (menghindari)
     Jika suatu risiko menghadirkan konsekuensi negatif yang tidak diinginkan, maka konsekuensi tersebut dapat dihindari sepenuhnya. Dengan menjauhi keterlibatan aktivitas bisnis atau membuat rancangan yang jauh dari penyebab risiko, terjadinya

peristiwa yang tidak diinginkan dapat dihindari. Salah satu cara untuk menghindari risiko adalah dengan keluar dari bisnis, membatalkan proyek, menutup pabrik, dll. Hal ini memang memiliki konsekuensi lain, namun ini merupakan opsi.

- Accept (menerima)
  Setiap produk yang dihasilkan memiliki peluang terbatas untuk gagal di tangan pelanggan. Saat resiko berada pada tingkat yang dapat diterima, tingkat kegagalan yang diperkirakan cukup rendah, maka kirimkan produk dan terima resikonya. Untuk kegagalan yang terkait dengan konsekuensi tinggi, pemantauan ketat kinerja lapangan pembangunan sistem peringatan dini merupakan tindakakn lebih bijaksana.
- Reduce/Control (mengurangi/mengendalikan)
  Jika tidak mungkin untuk mengurangi kejadian atau tingkat keparahan, menerapkan kontrol adalah pilihan. Kontrol yang dapat mendeteksi penyebab peristiwa yang tidak diinginkan sebelum konsekuensi yang terjadi selama penggunaan produk, atau mendeteksi akar penyebab kegagalan yang tidak diinginkan. Metode untuk mengurangi atau mengendalikan risiko adalah dengan melakukan diversifikasi. Melalui campuran produk, teknologi, pasar, operasi, dan rantai pasokan memungkinkan kemampuan tim untuk membatasi peluang berisiko tinggi ke tingkat yang dapat dikelola atau diterima.
- Transfer (memindahkan/mengalihkan)
  Strategi ini merupakan pengalihan beban konsekuensi risiko ke pihak lain. Bisa jadi termasuk menyerahkan beberapa kontrol, namun jika ada kesalahan, organisasi tidak bertanggung jawab. Cara konvensional untuk mentransfer risiko ke organisasi lain adalah dengan membeli asuransi. Ini mungkin memerlukan analisis yang cermat atas risiko dan probabilitas yang ada, namun merupakan pilihan yang layak dalam beberapa situasi.