Pembahasan UTS
Keamanan dan Jaminan Informasi 2023

Jawaban hanyalah sebuah referensi, belum tentu benar!

Made with ❤ By Diklat 2024

1. **Gambaran Umum Mengenai Security Wheel dan Hubungannya dengan 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.

2. **Contoh Ancaman pada Keamanan Informasi yang Disebabkan oleh:**

   a. Kegagalan Perangkat Lunak
      - Bug atau celah keamanan dalam aplikasi yang memungkinkan serangan oleh pihak luar.
      - Crash atau malfungsi sistem yang menyebabkan data hilang atau tidak dapat diakses.
      - Kegagalan update atau patch keamanan yang menyebabkan kerentanan sistem.

   b. Kegagalan SDM

- Kesalahan dalam pengolahan data, seperti salah memasukkan data nasabah atau transaksi.
- Kesalahan konfigurasi sistem yang membuat sistem rentan terhadap serangan.
- Kurangnya kesadaran atau pelatihan keamanan yang menyebabkan kebocoran data.

c. Faktor Eksternal
- Serangan siber dari peretas, seperti malware, phishing, atau serangan DDoS.
- Bencana alam seperti gempa bumi atau banjir yang merusak infrastruktur IT.
- Pemadaman listrik atau kegagalan jaringan yang menyebabkan gangguan layanan.

3. Tiga Unsur Penanggung Jawab Keamanan Informasi

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.

4. Studi Kasus Startup di Bidang Aplikasi Perangkat Lunak

a. Mengapa Kebijakan Informasi Itu Penting?

Kebijakan informasi membantu menjaga integritas, kerahasiaan, dan ketersediaan informasi perusahaan, serta melindungi dari ancaman eksternal.

b. Langkah-langkah dalam Kebijakan Informasi:
   5. Identifikasi aset informasi yang penting.
   6. Implementasi kontrol akses yang ketat.
   7. Pelatihan keamanan untuk karyawan.

c. Contoh Kebijakan Keamanan Level 2
   Penggunaan enkripsi untuk komunikasi data, otentikasi multi-faktor, dan pemantauan sistem secara real-time.

5. Upaya Perlindungan Fisik terhadap Keamanan Informasi

Salah satu upaya perlindungan fisik adalah dengan sistem deteksi intrusi, yang bertujuan untuk mendeteksi aktivitas yang mencurigakan di jaringan atau sistem. Contohnya termasuk:

a. CCTV: Mengawasi area sensitif.
b. Sensor Gerak: Memantau akses fisik yang tidak sah ke ruang server.
c. Akses Biometrik: Hanya memberikan akses kepada personel yang terautentikasi.

6. Studi Kasus PT Bank Sinarmas

PT Bank Sinarmas perlu mengidentifikasi aset kritis, risiko, dan pengendaliannya terhadap aset berikut:

a. Aset Hardware (printer teller, PIN pad, server, UPS, dsb.)
   Risiko:
   7. Kerusakan Fisik: Kerusakan atau kegagalan perangkat keras yang dapat mengganggu operasi.
   8. Pencurian atau Kehilangan: Perangkat keras dapat dicuri, yang memungkinkan akses tidak sah.
   9. Kerusakan Lingkungan: Seperti kebakaran atau banjir yang dapat merusak perangkat.

   Pengendalian:

   10. Keamanan Fisik: Menggunakan pengawasan CCTV dan akses terbatas ke area perangkat keras.
   11. Pemeliharaan Rutin: Menjadwalkan pemeliharaan untuk mencegah kerusakan.
   12. Redundansi: Memiliki perangkat cadangan untuk menghindari downtime.

b. Aset Software (Semua Software yang Digunakan di Bank)
   Risiko:
   13. Kerentanan Keamanan: Software yang tidak diperbarui dapat rentan terhadap serangan.
   14. Kesalahan Penggunaan: Pengguna mungkin tidak mengerti cara menggunakan software dengan benar.
   15. Serangan Malware: Software dapat terinfeksi malware yang merusak sistem.

   Pengendalian:

16. Pembaruan Berkala: Melakukan patching dan pembaruan untuk menutup kerentanan.
17. Pelatihan Pengguna: Memberikan pelatihan keamanan informasi kepada karyawan.
18. Antivirus dan Firewall: Menggunakan perangkat lunak antivirus dan firewall untuk melindungi sistem.

c. Aset Informasi (Identitas Nasabah, Nominal Nasabah, Password, Username, Data Transaksional)
Risiko:
19. Kebocoran Data: Data sensitif bisa bocor melalui peretasan atau insider threat.
20. Akses Tidak Sah: Data dapat diakses oleh pihak yang tidak berwenang.
21. Kehilangan Data: Data dapat hilang akibat kerusakan sistem atau kesalahan manusia.

Pengendalian:

22. Enkripsi Data: Melindungi data sensitif dengan enkripsi untuk mencegah akses tidak sah.
23. Otentikasi yang Kuat: Menerapkan sistem otentikasi yang kuat dan kontrol akses berbasis peran.
24. Audit dan Monitoring: Melakukan audit berkala untuk mendeteksi akses tidak sah.

d. Aset SDM (Teller, Customer Service, Staf TI)
Risiko:
25. Kesalahan Manusia: Karyawan dapat melakukan kesalahan dalam pengolahan data.
26. Insider Threat: Karyawan dapat membocorkan data atau melakukan tindakan merugikan.
27. Kurangnya Pelatihan: Staf yang tidak terlatih dapat meningkatkan risiko keamanan.

Pengendalian:

28. Pelatihan Rutin: Memberikan pelatihan keamanan informasi secara teratur kepada karyawan.
29. Kebijakan dan Prosedur: Menetapkan prosedur keamanan yang jelas dan mudah dipahami.
30. Audit dan Pemantauan: Melakukan audit berkala untuk memastikan kepatuhan terhadap kebijakan keamanan.