

TUGAS KEAMANAN INFORMASI



Disusun oleh:

INTAN PERMATASARI

1310651147

Kelas : D

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2015**

TUGAS 1

Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Jawab:

BAB 3 INFORMASI TATA KELOLA KEAMANAN MANAJEMEN RESIKO

Sebagai profesional keamanan informasi adalah untuk mengevaluasi resiko terhadap kritis kami aktif dan menyebarkan pengamanan untuk mengurangi resiko tersebut. Informasi tersebut bekerja dalam berbagai peran: api insinyur dinding, penguji penetrasi, auditor, manajemen, dll Benang merah adalah Risiko: itu adalah bagian dari deskripsi kerja. Keamanan Informasi Pemerintahan dan Manajemen Risiko domain berfokus pada Analisis risiko dan mitigasi. Domain ini juga detail tata keamanan atau struktur organisasi yang diperlukan untuk program keamanan informasi yang sukses. Perbedaan antara organisasi yang sukses dibandingkan dengan mereka yang gagal dalam hal ini alam biasanya tidak terikat dengan dolar atau ukuran staf: itu terkait dengan orang yang tepat di peran yang tepat. Staf keamanan informasi berpengetahuan dan berpengalaman dengan dukungan-ive dan kepemimpinan pribadi adalah kunci keberhasilan.

- Analisis Resiko

Semua profesional keamanan informasi menilai risiko melakukannya begitu sering sehingga menjadifkat kedua. Analisis Risiko akurat adalah keterampilan penting untuk keamanan informasi profesional. Kita harus menahan diri untuk standar yang lebih tinggi ketika menilai risiko. Aktiva Aktiva adalah sumber daya berharga Anda mencoba untuk melindungi. Aset dapat data, sistem, orang, bangunan, properti, dan sebagainya.

- Ancaman dan kerentanan

Sebuah ancaman adalah segala sesuatu yang berpotensi dapat menyebabkan kerusakan pada aset. ancaman termasuk gempa bumi, listrik padam, atau cacing berbasis jaringan. SEBUAH kerentanan adalah kelemahan yang memungkinkan ancaman untuk menyebabkan kerusakan. Contoh kerentanan (pencocokan ancaman kami sebelumnya) yang bangunan yang tidak dibangun untuk dengan- berdiri gempa bumi, pusat data tanpa daya cadangan yang tepat, atau Microsoft Windows sistem XP yang belum ditambah dalam beberapa tahun.

- Risiko = Ancaman 3 kerentanan

Untuk memiliki risiko, ancaman harus terhubung ke kerentanan. Hubungan ini dinyatakan oleh rumus:

Risiko ¼ ancaman
kerentanan

Anda dapat menetapkan nilai untuk risiko tertentu menggunakan formula ini. Menetapkan nomor untuk kedua

ancaman dan kerentanan. Kami akan menggunakan berbagai 1-5 (rentang adalah sewenang-wenang; hanya terus konsisten ketika membandingkan risiko yang berbeda).

- Matrix Analisis Risiko

Matrix Analisis Risiko menggunakan kuadran untuk memetakan kemungkinan risiko terjadi terhadap konsekuensi (atau dampak) risiko yang akan memiliki. Matrix Analisis Risiko memungkinkan Anda untuk melakukan Kualitatif Analisis Risiko (lihat bagian "Analisis Risiko Kualitatif dan Kuantitatif") Berdasarkan kemungkinan (dari "Langka" untuk "hampir pasti") dan konsekuensi (atau dampak), dari "tidak signifikan" untuk "Bencana." Skor yang dihasilkan rendah (L), sedang (M), tinggi (H), dan ekstrim risiko (E). Risiko rendah ditangani melalui proses normal, risiko moderat memerlukan mandat pemberitahuan pengelolaan, risiko tinggi memerlukan pemberitahuan manajemen senior.

- paparan Factor
paparan Factor (EF) adalah persentase nilai aset yang hilang akibat insiden. Dalam kasus laptop dicuri dengan tidak terenkripsi PII, Faktor Exposure adalah 100%: yang laptop dan semua data hilang.
- Tunggal Rugi Harapan (SLE) adalah biaya kerugian tunggal. SLE adalah Nilai Aktiva (AV) kali Factor Exposure (EF). Dalam kasus kami, SLE adalah \$ 25.000 (Nilai Aktiva) kali 100% (Exposure Factor) atau \$ 25.000.
- Tingkat tahunan Terjadinya (ARO) adalah jumlah kerugian Anda menderita per tahun.
Melihat melalui peristiwa masa lalu.
- Annualized Loss Expectancy (ALE) adalah biaya tahunan Anda karena risiko. Hal ini perhitungannya culated dengan mengalikan Harapan Loss Tunggal (SLE) kali Rate Tahunan Kejadian (ARO).
- Biaya Total Kepemilikan (TCO) adalah total biaya dari perlindungan yang meringankan. TCO menggabungkan biaya dimuka (sering biaya modal satu kali) ditambah biaya tahunan main- tenance, termasuk staf jam, biaya pemeliharaan penjual, langganan software, dll.
- panduan menjelaskan proses Analisis Risiko 9-langkah:
 1. sistem Karakterisasi
 2. ancaman Identifikasi
 3. kerentanan Identifikasi
 4. Analisis pengendalian
 5. Penentuan kemungkinan
 6. Analisis dampak

7. Penentuan risiko
8. kontrol Rekomendasi
9. hasil Dokumentasi

- **KEAMANAN INFORMASI TATA**

Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi: manajemen senior, kebijakan, proses, dan staf. Itu juga merupakan primer organisasi Sebagian Besar disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil program keamanan.

Kebijakan keamanan dan dokumen terkait Dokumen seperti kebijakan dan prosedur adalah bagian yang diperlukan dari setiap sukses program keamanan informasi. Dokumen-dokumen ini harus didasarkan pada realitas: mereka tidak dokumen idealis yang duduk di rak-rak mengumpulkan debu. Mereka harus mencerminkan dunia nyata dan memberikan bimbingan pada benar.

Polis Kebijakan yang arahan manajemen tingkat tinggi. Kebijakan adalah wajib: jika Anda tidak setuju dengan kebijakan pelecehan seksual perusahaan Anda, misalnya, Anda tidak memiliki pilihan untuk tidak mengikutinya.

- Vendor, konsultan, dan kontraktor
keamanan dapat memperkenalkan risiko organisasi. Mereka adalah karyawan tidak langsung dan kadang-kadang memiliki akses ke sistem di beberapa-organisasi organisasi-. Jika dibiarkan, mereka dapat menempatkan data sensitif organisasi pada perangkat tidak dikontrol (atau dijamin) oleh organisasi. Personil pihak ketiga dengan akses ke data sensitif harus dilatih dan dibuat menyadari risiko, seperti karyawan.
- Outsourcing dan offshoring outsourcing
adalah penggunaan pihak ketiga untuk menyediakan dukungan teknologi informasi layanan yang sebelumnya dilakukan di rumah. Offshoring outsourcing untuk negara lain. Keduanya dapat menurunkan total biaya kepemilikan dengan menyediakan layanan TI dengan biaya lebih rendah. Mereka juga dapat meningkatkan sumber daya teknologi informasi dan keterampilan set dan sumber daya yang tersedia untuk perusahaan (terutama perusahaan kecil), yang dapat meningkatkan kerahasiaan, integritas, dan ketersediaan data. Sebuah Analisis Risiko menyeluruh dan akurat harus dilakukan sebelum outsourcing atau data sensitif offshoring. Jika data akan berada di negara lain, Anda harus memastikan bahwa hukum dan peraturan yang mengatur data diikuti, bahkan di luar yurisdiksi mereka.

TUGAS 2

Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan teman-temennya.

Jawaban :

Tentang Aplikasi AntiVirus

Pada Blog ini saya akan menampilkan beberapa aplikasi software antivirus yang bagus untuk segala jenis PC/Laptop.

Cekidot :



1.Norton Internet Security

Norton AntiVirus TM 2013 - Antivirus, yang menyediakan perlindungan dasar yang kuat dan cepat terhadap virus dan spyware. Versi baru yang lebih cepat dan lebih handal.

Dengan pengguna Norton AntiVirus dengan alat efektif yang tersedia untuk on-demand scanning antivirus, perlindungan yang kuat secara real time, serta fungsi pendukung banyak lainnya untuk keamanan komputer dan informasi.

Norton AntiVirus dengan menggunakan teknologi inovatif untuk melawan virus terbaru dan ancaman berbahaya lainnya tanpa memperlambat komputer Anda. Informasi lebih lanjut tentang Norton Internet Security 2013

Norton Internet Security 2013 - menyediakan perlindungan cepat dan mudah melawan ancaman online. Terpadu antivirus dan firewall melindungi komputer Anda, jaringan lokal, aktivitas online dan informasi pribadi Anda, dengan menggunakan teknologi inovatif untuk menangani ancaman agresif modern. kuat dan cepat perlindungan terhadap malware dan ancaman online tanpa memperlambat komputer Anda. Peningkatan Norton Protection System dengan multi-tingkat teknologi keamanan yang bekerja sama untuk memberikan perlindungan komprehensif.

Norton Internet Security 2013 - perlindungan yang kuat dan cepat terhadap malware dan ancaman online tanpa memperlambat komputer Anda. Fungsi dari antivirus, antispyware, firewall dilengkapi teknologi unik untuk secara efektif melindungi komputer Anda dari semua jenis ancaman Internet.

[klik disini untuk DOWNLOAD\](#)

2.PCMAV

PCMedia AntiVirus disingkat PCMAV adalah perangkat lunak antivirus buatan PCMedia, sebuah majalah komputer Indonesia. Beroperasi dibawah sistem operasi Microsoft Windows (XP/Vista/7 keatas). PC Media Antivirus (PCMAV) sendiri bukan merupakan satu-satunya antivirus di Indonesia yang mempunyai formula atau teknologi khusus untuk mengatasi virus komputer yang menyebar luas di masyarakat, baik jenis lokal maupun mancanegara (asing), akan tetapi sejauh ini PCMAV digadang-gadang dapat membersihkan infeksi terhadap secara akurat dan tuntas hingga pulih 100%.

Dikarenakan menggunakan bahasa pemrograman Delphi, menjadikannya berbeda dengan antivirus standar industri sejenis yang biasanya menggunakan bahasa pemrograman Microsoft Visual C++. Untuk virus database-nya sendiri dikarenakan virus database internal-nya masih sedikit, PCMAV juga memanfaatkan penggunaan alternatif database dari ClamAV sebagai database tambahan eksternal.

klik disini untuk [DOWNLOAD](#)

3. Avira

Avira AntiVir Personal – Free Antivirus merupakan salah satu Software Antivirus yang bukan tidak punya kelemahan, berdasarkan pengalaman saya kebanyakan file crack-patch-serial number beberapa software (bajakan kali...hehehe) mengandung virus dan oleh Avira di-eksekusi secara delete dan tidak diperbaiki (apa juga karena free-gratis itu? Dan bukan Premium). Apapun itu, sepertinya lebih baik virus di delete daripada melihara virus di komputer kita. (karena saya kurang begitu paham enskripsi sebuah virus bekerja).

Memang tidak ada antivirus terbaik atau terburuk di dunia komputer dan internet, meskipun software antivirus kita kapasitasnya kecil dan gratisan tapi kita rajin update, pasti akan bekerja maksimal. Dan sebaliknya jika antivirus kita berbayar dan berlisensi tapi definisi virus-nya tidak pernah di-update...saat ada virus masuk, anda harus siap kehilangan data dan selamat install ulang OS Windows-nya!

klik disini untuk [DOWNLOAD](#)

Aplikasi terkait :

- a. AVG Free klik disini untuk [DOWNLOAD](#)
- b. Norton 360 klik disini untuk [DOWNLOAD](#)
- c. Nod32 klik disini untuk [DOWNLOAD](#)

Sekian informasi sederhana saya mengenai Contoh Software Aplikasi ANTIVIRUS yang dapat saya berikan, semoga teman - teman semua dapat mengerti dan menambah pengetahuan mengenai beberapa Contoh Software Aplikasi.