NAMA : NIKMATUS SHOLEHA

NIM : 1310651097

KELAS: E

Kebijakan melidungi CIA PII oleh pengerasan operasi system

- Keamanan informasi pemerintahan

Manajemen senior menciptakan program keamanan informasi dan memastikan bahwa itu benar di kelola dan di danai dan memiliki prioritas organisasi.

Pemilik data juga di sebut pemilik informasi atau pemilik bisris adalah pengelola sesuatu ment karyawan bertanggung jawab untuk memastikan bahwa data yang spesifik dilindungi. Pemilik data menentukan data label sensitivitas dan frekuensi backup data. Sebuah perusahaan dengan beberapa lini bisnis mungkin memiliki beberapa pemilik data. Pemilik data melakukan tugas manajemen; kustodian melakukan hands-on perlindungan data.

Mereka melakukan
backup data dan pemulihan, sistem patch, mengkonfigurasi perangkat lunak antivirus, dll Penjaga mengikuti perintah rinci; mereka tidak membuat keputusan penting tentang bagaimana data dilindungi. Pemilik data dapat menentukan "Semua data harus didukung setiap 24 jam. "The penjaga (dan manajer mereka) maka akan menyebarkan dan mengoperasikan solusi backup yang memenuhi persyaratan pemilik data itu.

Pemeriksaan latar belakang
Organisasi harus melakukan pemeriksaan latar belakang menyeluruh sebelum mempekerjakan orang.Seorang kriminal catatan cek harus dilakukan, dan semua pengalaman, pendidikan, dan sertifikasi harus diverifikasi. Berbohong atau melebih-lebihkan tentang pendidikan, sertifikasi yang tions, dan kredensial terkait adalah salah satu contoh yang paling umum dari ketidakjujuran dalam hal proses perekrutan.
Lebih pemeriksaan latar belakang menyeluruh harus dilakukan untuk peran dengan tinggi hak istimewa, seperti akses ke uang atau informasi rahasia. Pemeriksaan ini dapat termasuk penyelidikan keuangan, catatan kriminal yang lebih menyeluruh memeriksa, dan antar pandangan dengan teman-teman, tetangga, dan rekan kerja saat ini dan mantan.

Pelatihan keamanan mengajarkan pengguna bagaimana melakukan sesuatu. Contohnya termasuk pelatihan personil meja bantuan baru untuk membuka, memodifikasi, dan tiket layanan dekat; jaringan pelatihan insinyur untuk mengkonfigurasi router; atau pelatihan administrator keamanan untuk membuat baru akun.

Keamanan informasi praktek terbaik adalah konsensus cara terbaik untuk melindungi con yang fidentiality, integritas, dan ketersediaan aset. Mengikuti praktik terbaik adalah cara untuk menunjukkan hati-hati dan due diligence.

Keamanan Informasi Pemerintahan
ISO 17799 dan ISO seri 27000
ISO17799wasabroad-basedapproachforinformationsecuritycodeofpracticebythe Organisasi Internasional untuk Standardisasi (berbasis di Jenewa, Swiss). Itu Judul lengkap adalah "ISO / IEC 17799: 2005 teknologi Keamanan Informasi Techniques-
Kode Praktek untuk Manajemen Keamanan Informasi "ISO 17799:. 2005 menandakan versi standar 2005. Hal ini didasarkan pada BS (British Standard) 7799 Part 1.
FAKTA CEPAT
ISO 17799 memiliki 11 daerah, dengan fokus pada kontrol keamanan informasi spesifik:

1.Polis
2.Organisasi keamanan informasi
3.Manajemen aset
4.Keamanan sumber daya manusia
5.Keamanan fisik dan lingkungan
6.Komunikasi dan manajemen operasi
7.Kontrol akses
8.Akuisisi sistem informasi, pengembangan, dan pemeliharaan
9.Pengelolaan insiden keamanan informasi
10.Manajemen kelangsungan bisnis
11.Pemenuhan

- ❖ Peningkatan Pelayanan terus-menerus

- ➢ Layanan Strategi membantu TI memberikan layanan
- ➢ Layanan Desain detail infrastruktur dan arsitektur yang dibutuhkan untuk memberikan layanan TI
- ➢ Layanan Transisi menggambarkan mengambil newprojectsandmakingthemoperational.ServiceOperationcoversIToperationscon-Trols. Akhirnya, terus menerus Peningkatan Pelayanan menjelaskan cara untuk meningkatkan TI yang ada jasa.

NIST SP 800-37 menjelaskan Sertifikasi empat langkah dan proses Akreditasi:
• Fase inisiasi
• Fase sertifikasi keamanan
• Fase akreditasi keamanan
• Terus menerus fase pemantauan
Sistem keamanan informasi dan rencana mitigasi risiko yang diteliti selama inisiasi tiationphase.Thesecurityofthesystemisassessedanddocumentedduringthesecurity fase sertifikasi. Keputusan untuk menerima risiko yang diwakili oleh sistem yang dibuat dan didokumentasikan selama fase akreditasi keamanan. Akhirnya, setelah terakreditasi, yang keamanan yang sedang berlangsung dari sistem diverifikasi selama fase pemantauan terus menerus.