Keamanan Informasi

Nama: Ahmad rafi aziz

Nim: 1310651145

INFORMASI TATA KEAMANAN

(Information Security Governance)

Information Security Governance atau yang disbut engan informasi tata keamanaan adalah keamanan informasi di tingkat organisasi: manajemen senior, kebijakan, proses, dan staf, disediakan oleh kepemimpinan senior, yang diperlukan untuk program keamanan informasi yang sukses.

komponen-komponen dasar:

• Tujuan • Lingkup • Tanggung Jawab • Kepatuhan

Tanggung jawab termasuk tanggung jawab dari tim staf keamanan informasi, kebijakan dan manajemen, serta tanggung jawab semua anggota organisasi.

Prosedur Prosedur adalah langkah-demi-langkah panduan untuk menyelesaikan tugas. Mereka tingkat rendah dan spesifik. Seperti kebijakan, prosedur wajib. Berikut ini adalah contoh prosedur sederhana untuk membuat user baru:

1. Menerima formulir permintaan baru-pengguna dan memverifikasi kelengkapan.

2. Pastikan bahwa manajer pengguna telah menandatangani formulir.

3. Pastikan bahwa pengguna telah membaca dan setuju dengan kebijakan keamanan akun pengguna.

4. Klasifikasikan peran pengguna dengan mengikuti prosedur peran-tugas NX-103.

5. Pastikan bahwa pengguna telah memilih "kata rahasia," seperti nama gadis ibu mereka, dan masukkan ke dalam profil akun help desk. 6. Buat account dan menetapkan peran yang tepat.

7. Menetapkan kata rahasia sebagai password awal dan mengatur "pengguna Force untuk mengubah password pada login berikutnya untuk 'Benar'."

8. E-mail dokumen Akun Baru ke pengguna dan manajer mereka.

Langkah-langkah dari prosedur ini adalah wajib. Administrator keamanan tidak memiliki pilihan untuk melewatkan langkah 1, misalnya, membuat akun tanpa formulir.

Standar Sebuah standar menggambarkan penggunaan khusus dari teknologi, sering diterapkan untuk perangkat keras dan perangkat lunak. "Semua karyawan akan menerima ACME Nexus-6 laptop dengan 4 gigabyte memori, 2,8 GHZ dual core CPU, dan 2-Terabyte disk" adalah contoh dari standar hardware. "Laptop akan menjalankan Windows 8 Enterprise, versi 64-bit" adalah contoh dari perangkat lunak

Peran dan tanggung jawab peran keamanan informasi primer meliputi manajemen senior, pemilik data, kustodian, dan user. Setiap memainkan peran yang berbeda dalam mengamankan aset organisasi.

Manajemen senior menciptakan program keamanan informasi dan memastikan bahwa itu benar dikelola dan didanai dan memiliki prioritas organisasi. Hal ini bertanggung jawab untuk memastikan bahwa semua aset organisasi dilindungi. Pemilik data (juga disebut pemilik informasi atau pemilik bisnis) adalah karyawan manajemen bertanggung jawab untuk memastikan bahwa data yang spesifik dilindungi. Pemilik Data menentukan data yang 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. Sebuah kustodian memberikan hands-on perlindungan aset seperti data. Mereka melakukan data backup 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 cadangan yang memenuhi persyaratan pemilik data itu. Pengguna adalah peran informasi utama keamanan keempat. Pengguna harus mengikuti aturan: mereka harus mematuhi kebijakan wajib prosedur, standar, dll Mereka tidak harus menulis password mereka turun atau rekening saham, misalnya. Pengguna harus dibuat sadar risiko ini dan persyaratan. Anda tidak bisa menganggap mereka akan tahu apa yang harus dilakukan atau menganggap mereka sudah melakukan hal yang benar: mereka harus diberitahu, melalui kesadaran keamanan informasi.

Pengguna keamanan personil dapat menimbulkan risiko keamanan terbesar untuk sebuah organisasi. Pemeriksaan latar belakang harus dilakukan, kontraktor harus aman dikelola, dan pengguna harus dilatih dengan baik dan dibuat sadar risiko keamanan, seperti yang akan kita bahas selanjutnya. Kontrol seperti Perjanjian Menyingkap (NDA) dan perjanjian kerja terkait yang direkomendasikan kontrol keamanan personil.

Karyawan pemutusan Pemutusan harus menghasilkan pencabutan segera semua akses karyawan. Di luar rekening pencabutan, pemutusan harus menjadi proses yang adil. Ada alasan etika dan hukum untuk mempekerjakan pemutusan adil, tetapi ada juga informasi tambahan

Keuntungan keamanan.

Musuh terburuk organisasi dapat menjadi mantan karyawan yang tidak puas, yang, bahkan tanpa akses account yang sah, tahu di mana "titik-titik lemah yang."

Kesadaran keamanan dan kesadaran pelatihan Keamanan dan pelatihan sering bingung. Kesadaran perubahan perilaku pengguna; pelatihan menyediakan keahlian. Mengingatkan pengguna untuk tidak pernah berbagi account atau menulis password mereka turun adalah contoh dari kesadaran. Hal ini diasumsikan bahwa beberapa pengguna melakukan hal yang salah, dan kesadaran dirancang untuk mengubah perilaku itu. Pelatihan keamanan mengajarkan pengguna bagaimana melakukan sesuatu. Contohnya termasuk pelatihan personil meja bantuan baru untuk membuka, memodifikasi, dan tiket

layanan dekat; insinyur jaringan pelatihan untuk mengkonfigurasi router; atau pelatihan administrator keamanan untuk membuat account baru.

Vendor, konsultan, dan kontraktor keamanan Vendor, konsultan, dan kontraktor dapat memperkenalkan risiko organisasi. Mereka adalah karyawan tidak langsung dan kadang-kadang memiliki akses ke sistem di beberapa 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 sadar risiko, seperti karyawan. Pemeriksaan latar belakang juga mungkin diperlukan, tergantung pada tingkat akses yang diperlukan. Kebijakan keamanan informasi, prosedur, dan bimbingan lainnya harus diterapkan juga. Kebijakan tambahan mengenai kepemilikan data dan kekayaan intelektual harus dikembangkan. Aturan yang jelas mendikte mana dan kapan pihak ketiga dapat mengakses atau menyimpan data harus dikembangkan.

Outsourcing dan offshoring Outsourcing adalah penggunaan pihak ketiga untuk menyediakan layanan dukungan teknologi informasi yang sebelumnya dilakukan di rumah. Offshoring outsourcing ke 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 offshoring sensitivedata.If data akan residein anothercountry, youmustensure bahwa hukum dan peraturan yang mengatur data diikuti, bahkan di luar yurisdiksi mereka.

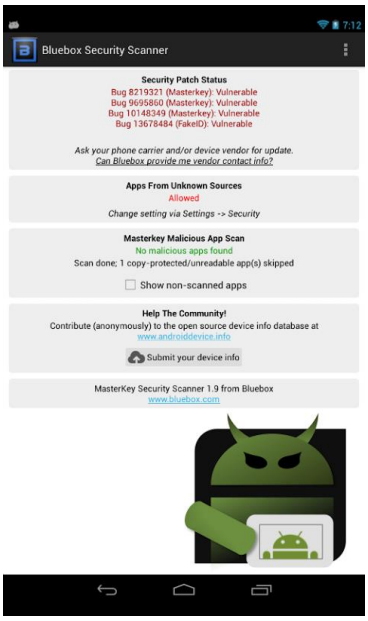
Privasi Privasi adalah perlindungan kerahasiaan informasi pribadi. Banyak organizationshostpersonalinformationabouttheirusers: PIIsuchassocialsecuritynumbers, informasi keuangan seperti informasi gaji dan rekening bank tahunan

diperlukan untuk deposito penggajian, dan informasi kesehatan untuk tujuan asuransi. Kerahasiaan informasi ini harus terjamin.

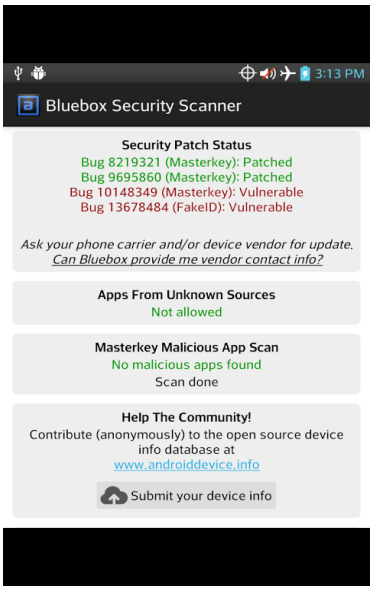
Kelalaian kelalaian Gross Gross adalah kebalikan dari perawatan karena. Ini adalah konsep hukum yang penting. Jika Anda menderita kerugian dari PII, tetapi dapat menunjukkan hati dalam melindungi PII, Anda berada di tanah secara hukum kuat, misalnya. Jika Anda tidak dapat menunjukkan hati-hati (Anda terlalu lalai), Anda berada dalam posisi hukum jauh lebih buruk.

Terbaik Informasi praktik keamanan praktek terbaik adalah konsensus cara terbaik untuk melindungi kerahasiaan, integritas, dan ketersediaan aset. Mengikuti praktik terbaik adalah cara untuk menunjukkan hati-hati dan due diligence.

Bluebox Security Scanner



Bluebox Security Scanner adalah aplikasi yang digunakan untuk memeriksa apakah ada vulnerability pada ponsel berperangkat Android anda. Pengecakan melalui aplikasi ini karena ada beberapa celah keamanan yang terdapat pada perangkat Android anda. Aplikasi ini juga dapat mengecek apakah perangkat anda dapat melakukan penginstalan aplikasi dari "Unknown Source" yang memungkinkan dapat mengeksploitasi vulnerability pada perangkat anda.



Scanner bluebox Security akan memindai perangkat Anda untuk menentukan:
- Jika sistem Anda rentan atau patch ke salah satu "Palsu ID" atau "Master Key" kelemahan keamanan yang mempengaruhi perangkat Android
- Jika pengaturan sistem Anda mengizinkan aplikasi 'Sumber Untrusted' menginstal
- Jika ada aplikasi yang diinstal pada perangkat Anda sedang mencoba untuk jahat mengambil keuntungan dari setiap kelemahan keamanan 'Master Key'