Domain 1 Acces Control

CORNERSTONE KONSEP KEAMANAN INFORMASI

Sebelum kita bisa menjelaskan kontrol akses, kita harus mendefinisikan konsep keamanan informasi landasan. Konsep-konsep ini memberikan fondasi yang 10 domain Badan Umum Pengetahuan dibangun.

Kerahasiaan, integritas, dan ketersediaan

Kerahasiaan, Integritas, dan Ketersediaan adalah "triad CIA," konsep landasan keamanan informasi. Triad, yang ditunjukkan pada Gambar 1.1, membentuk bangku berkaki tiga keamanan informasi dibangun di atas. Urutan akronim dapat berubah (beberapa lebih suka "AIC," mungkin untuk menghindari hubungan dengan badan intelijen tertentu), tetapi konsep sangat penting. Buku ini akan menggunakan "CIA" singkatan

Kerahasiaan

Kerahasiaan berusaha untuk mencegah pengungkapan yang tidak sah informasi: itu membuat data rahasia. Dengan kata lain, kerahasiaan berusaha untuk mencegah akses tidak sah ke data membaca. Contoh dari serangan kerahasiaan akan pencurian informasi pribadi (PII), seperti informasi kartu kredit

Ada dua jenis integritas: integritas data dan integritas sistem. Integritas data berusaha untuk melindungi informasi terhadap modifikasi yang tidak sah; integritas sistem berusaha untuk melindungi sistem, seperti sistem operasi Windows server 2012, dari modifikasi yang tidak sah.

Ketersediaan Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan aDenial-of-Service (DoS) serangan, yang berusaha layanan todeny (atau ketersediaan) dari suatu sistem.

Pengungkapan, perubahan, dan perusakan CIA triad juga dapat dijelaskan oleh kebalikannya: Pengungkapan, Perubahan, dan Destruction (DAD). Pengungkapan adalah pengungkapan yang tidak sah informasi; perubahan adalah modifikasi yang tidak sah dari data, dan kehancuran yang membuat sistem tidak tersedia. Sementara singkatan CIA kadang-kadang berubah, singkatan DAD ditunjukkan dalam urutan itu.

Identitas dan otentikasi, otorisasi, dan akuntabilitas Istilah "AAA" sering digunakan, menggambarkan konsep landasan Otentikasi, Otorisasi, dan Akuntabilitas. Waktu keluar dari singkatan AAA adalah Identifikasi, yang diperlukan sebelum tiga "A" dapat mengikuti.

Sekarang kita telah meninjau konsep kontrol akses landasan, kita bisa mendiskusikan model kontrol akses yang berbeda: model utama adalah Discretionary Access Control (DAC), Wajib Access Control (MAC), dan kontrol akses nondiscretionary.

MODEL ACCESS CONTROL

Kontrol akses discretionary Discretionary Access Control (DAC) memberikan pelajaran kontrol penuh dari benda-benda yang mereka telah diberi akses ke, termasuk berbagi objek dengan mata pelajaran lain. Subyek diberdayakan dan mengendalikan data mereka. Sistem operasi standar UNIX dan Windows menggunakan DAC untuk sistem berkas: subjek dapat memberikan pelajaran lain akses ke file mereka, mengubah atribut mereka, mengubah mereka, atau menghapusnya.

Kontrol akses wajib Access Wajib Control (MAC) adalah sistem-ditegakkan kontrol akses berdasarkan izin subjek dan label objek. Subjek dan objek memiliki izin dan label, masing-masing, seperti rahasia, rahasia, dan rahasia. Subjek A dapat mengakses sebuah objek hanya jika izin subjek sama dengan atau lebih besar dari label objek. Subyek tidak dapat berbagi objek dengan mata pelajaran lain yang tidak memiliki izin yang tepat atau "menulis" objek untuk tingkat klasifikasi yang lebih rendah (seperti dari rahasia untuk rahasia). Sistem MAC biasanya terfokus pada menjaga kerahasiaan data.

Kontrol akses nondiscretionary Peran Berbasis Access Control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem yang didasarkan pada peran subjek. Peran A bisa menjadi perawat, administrator cadangan, teknisi bantuan meja, dll Subyek dikelompokkan menjadi peran dan peran masing-masing didefinisikan memiliki izin akses berdasarkan peran, bukan individu. RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak dapat mentransfer objek untuk mata pelajaran lainnya. Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain, terkait dengan RBAC. Kontrol akses tugas berbasis didasarkan pada tugas masing-masing harus tunduk

Kontrol akses terpusat kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Alih-alih menggunakan database kontrol akses lokal, sistem otentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk memberikan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem. Kontrol akses terpusat terpusat dapat memberikan tiga "A" dari kontrol akses: Otentikasi, Otorisasi, dan Akuntabilitas.

Protokol kontrol akses dan kerangka model Kedua sentralisasi dan desentralisasi dapat mendukung pengguna jauh otentikasi ke sistem lokal. Sejumlah protokol dan kerangka kerja dapat digunakan untuk mendukung kebutuhan ini, termasuk RADIUS, Diameter, TACACS / TACACSþ, PAP, dan CHAP. RADIUS Remote Authentication Dial-In Service Pengguna (RADIUS) protokol adalah sistem otentikasi pihak ketiga. RADIUS menggunakan User Datagram Protocol (UDP) port 1812 (otentikasi) dan 1813 (akuntansi). RADIUS dianggap sebagai "AAA" sistem, yang terdiri dari tiga komponen: otentikasi, otorisasi, dan akuntansi. Ini mengotentikasi kredensial subjek terhadap database otentikasi. Ini kewenangan pengguna dengan memungkinkan akses pengguna tertentu 'untuk objek data tertentu. Hal ini menyumbang setiap sesi data dengan membuat entri log untuk setiap koneksi RADIUS dibuat.

Diameter Diameter adalah RADIUS 'penerus, dirancang untuk memberikan Otentikasi ditingkatkan, Otorisasi, dan Akuntansi (AAA) kerangka. RADIUS memberikan akuntabilitas terbatas dan memiliki masalah dengan fleksibilitas, skalabilitas, kehandalan, dan keamanan. Diameter lebih fleksibel, yang memungkinkan dukungan bagi pengguna jarak jauh ponsel, misalnya.

TACACS dan TACACS1 The Terminal Access Controller Access Control System (TACACS) adalah sistem kontrol akses terpusat yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi. TACACS menggunakan port UDP 49 (dan mungkin juga menggunakan TCP). Password dapat digunakan kembali memiliki kerentanan keamanan: TACACSþ ditingkatkan memberikan proteksi password yang lebih baik dengan memungkinkan otentikasi dua faktor yang kuat. TACACSþ tidak kompatibel dengan TACACS. TACACSþ menggunakan port TCP 49 untuk otentikasi dengan TACACSþserver.

ACCESS CONTROL KATEGORI

Dalam rangka untuk memahami dan tepat menerapkan kontrol akses, memahami apa manfaat setiap kontrol dapat menambah keamanan sangat penting. Pada bagian ini, setiap jenis accessControl akan ditentukan pada thebasis ofhowitaddsto keamanan tersebut yang sistem. Ada enam jenis kontrol akses:

• Pencegahan • Detektif • Korektif • Pemulihan • jera • Kompensasi

Jenis kontrol akses ini dapat jatuh ke dalam salah satu dari tiga kategori: administrasi, teknis, dan fisik.

1. Administrasi (juga disebut directive) kontrol dilaksanakan dengan menciptakan dan mengikuti kebijakan organisasi, prosedur, atau peraturan. Pelatihan pengguna dan kesadaran juga termasuk dalam kategori ini.

2. kontrol Teknis diimplementasikan menggunakan perangkat lunak, perangkat keras, atau firmware yang membatasi akses logis pada sistem teknologi informasi. Contohnya termasuk firewall, router, dan enkripsi.

3. kontrol fisik diimplementasikan dengan perangkat fisik, seperti kunci, pagar, gerbang, dan penjaga keamanan.

Kontrol pencegahan preventif mencegah tindakan dari terjadi. Ini berlaku pembatasan apa pengguna potensial, baik resmi atau tidak sah, dapat dilakukan. Contoh dari

Kategori dan Jenis Access Kontrol Defensive

Kontrol pencegahan administrasi adalah skrining obat pra kerja. Hal ini dirancang untuk mencegah sebuah organisasi dari mempekerjakan seorang karyawan yang menggunakan obat-obatan terlarang.

Kontrol Detektif Detektif adalah kontrol yang siaga selama atau setelah serangan yang berhasil. Sistem deteksi intrusi memperingatkan setelah serangan sukses, kamera televisi sirkuit tertutup (CCTV) yang penjaga waspada terhadap penyusup, dan bangunan sistem alarm yang dipicu oleh penyusup merupakan contoh dari kontrol detektif.

Kontrol korektif korektif bekerja dengan "memperbaiki" sistem atau proses rusak. Kontrol akses korektif biasanya bekerja bergandengan tangan dengan kontrol akses detektif. Perangkat lunak antivirus memiliki kedua komponen. Pertama, perangkat lunak antivirus berjalan scan dan menggunakan itsdefinitionfiletodetectwhetherthereisanysoftwarethatmatches itsviruslist.Ifit mendeteksi virus, kontrol korektif mengambil alih, menempatkan perangkat lunak yang mencurigakan di karantina, atau menghapusnya dari sistem.

Pemulihan Setelah insiden keamanan telah terjadi, kontrol pemulihan mungkin perlu diambil untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih: diinstal ulang dari OS Media atau gambar, data dikembalikan dari backup, dll

Jera Deterrentcontrolsdeterusersfromperformingactionsonasystem.Examplesincludea "Waspadalah terhadap anjing" tanda: pencuri menghadapi dua bangunan, satu dengan anjing penjaga dan satu tanpa, ismorelikelytoattackthebuildingwithoutguarddogs.Alargefineforspeedingis jera bagi pengemudi untuk tidak mempercepat. Sebuah kebijakan sanksi yang membuat pengguna memahami bahwa mereka akan dipecat jika mereka tertangkap situs Web berselancar terlarang atau ilegal adalah pencegahan.

Kompensasi Sebuah kontrol kompensasi adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengimbangi kelemahan dalam kontrol lainnya.

METODE AUTHENTIKASI Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan otentikasi yang tepat dari mata pelajaran dalam sistem IT. Subjek A pertama mengidentifikasi dirinya; Identifikasi ini tidak bisa dipercaya. Subjek kemudian mengotentikasi dengan identitas providinganassurancethattheclaimed isvalid.Acredentialsetisthetermused untuk kombinasi keduanya identifikasi dan otentikasi pengguna.

metode dasar otentikasi

Ada tiga metode dasar otentikasi: Tipe 1 (sesuatu yang Anda tahu), Tipe 2 (sesuatu yang harus Anda), dan Tipe 3 (sesuatu yang Anda). Tipe keempat otentikasi beberapa tempat Anda.

Otentikasi kuat (juga disebut otentikasi multifaktor) mensyaratkan bahwa saat ini pengguna lebih dari satu faktor otentikasi. Sebagai contoh, pengguna dapat memiliki kartu ATM untuk menarik uang dari bank, tapi ia / dia juga harus memasukkan PIN yang benar.

Ketik 1 otentikasi: sesuatu yang Anda tahu Ketik 1 otentikasi (sesuatu yang Anda tahu) membutuhkan pengujian subyek dengan semacam tantangan dan respon dimana subjek harus merespon dengan jawaban berpengetahuan. Subjek diberikan akses atas dasar sesuatu yang mereka tahu, seperti password atau PIN (Personal Identification Number, password nomor-based). Ini adalah bentuk paling mudah, dan sering lemah, otentikasi.

Sandi Sandi telah menjadi landasan untuk kontrol akses ke sistem TI. Mereka relatif mudah dan murah untuk melaksanakan. Banyak online banking, layanan portofolio saham, Web mail pribadi, dan kesehatan sistem masih menggunakan nama pengguna dan password sebagai metode kontrol akses. Ada empat jenis password untuk dipertimbangkan ketika menerapkan kontrol akses: password statis, passphrase, satu kali password, dan password dinamis. Password statis password dapat digunakan kembali yang mungkin atau mungkin tidak berakhir. Mereka biasanya user-generated dan bekerja dengan baik ketika dikombinasikan dengan jenis otentikasi lain, seperti kartu pintar atau kontrol biometrik. Passphrase adalah password statis panjang, terdiri dari kata-kata dalam frase atau kalimat. Contoh passphrase adalah: "Aku akan lulus CISSP® dalam 6 bulan!" Passphrases dapat dibuat lebih kuat dengan menggunakan kata-kata omong kosong (menggantikan CISSP® dengan "xyzzy" di passphrase sebelumnya, misalnya), dengan mencampurkan kasus, dan dengan menggunakan angka dan simbol tambahan. Satu kali password dapat digunakan untuk otentikasi tunggal. Mereka sangat aman tapi sulit

untuk mengelola. Sebuah password satu kali tidak mungkin untuk menggunakan kembali dan berlaku hanya untuk satu kali penggunaan. Password dinamis berubah secara berkala. RSA keamanan membuat perangkat tanda sinkron disebut SecurID yang menghasilkan kode token baru setiap 60 detik. Pengguna menggabungkan PIN statis mereka dengan RSA dinamis kode token untuk membuat satu password yang dinamis yang berubah setiap kali digunakan. Salah satu kelemahan bila menggunakan password yang dinamis adalah biaya token sendiri.

Authentication Metode

Sandi hash dan password cracking Dalam kebanyakan kasus, password teks yang jelas tidak disimpan dalam sistem IT; hanya output hash dari mereka password yang disimpan. Hashing adalah satu arah enkripsi menggunakan algoritma dan tidak ada tombol. Ketika pengguna mencoba untuk login, password mereka mengetik hash, dan hash yang dibandingkan terhadap hash yang disimpan pada sistem. Fungsi hash tidak dapat dibalik: tidak mungkin untuk membalikkan algoritma dan menghasilkan password dari hash. Sementara hash tidak dapat terbalik, penyerang dapat menjalankan algoritma hash maju berkali-kali, memilih berbagai password mungkin dan membandingkan output ke hash yang diinginkan, berharap menemukan kecocokan (dan untuk mendapatkan password asli). Ini disebut password cracking.

Serangan kamus Sebuah serangan kamus menggunakan daftar kata: daftar standar dari kata-kata, dan kemudian berjalan setiap kata melalui algoritma hash. Jika perangkat lunak retak sesuai dengan output dari serangan keluaran kamus hash password, penyerang akan dapat mengidentifikasi password asli.

Serangan Hybrid Sebuah serangan hybrid menambahkan, prepends, atau perubahan karakter dalam kata-kata dari kamus sebelum hashing, untuk mencoba celah tercepat password yang kompleks. Sebagai contoh, seorang penyerang mungkin memiliki kamus potensi password administrator sistem, tetapi juga menggantikan setiap huruf "o" dengan angka "0"

Serangan brute-force Brute-forceattackstake lebih banyak waktu Butare lebih penyerang effective.The menghitung output hash untuk setiap password mungkin. Hanya beberapa tahun yang lalu, kecepatan komputer dasar masih cukup lambat untuk membuat tugas yang menakutkan. Namun, dengan kemajuan dalam kecepatan CPU dan komputasi paralel, waktu yang diperlukan untuk brute-force password yang kompleks telah jauh berkurang.

Tabel pelangi

adalah kompilasi precomputed dari plainteks dan matchingciphertexts (biasanya password dan hash cocok mereka). Tabel pelangi sangat mempercepat banyak jenis password cracking serangan, sering mengambil menit untuk memecahkan mana metode lain (seperti kamus, hibrida, dan password brute force retak upaya) mungkin memakan waktu lebih lama. Meskipun tabel pelangi bertindak sebagai database, mereka lebih kompleks di bawah tenda, bergantung pada waktu / memori trade-off untuk mewakili dan memulihkan password dan hash. Kebanyakan tabel pelangi dapat memecahkan sebagian besar, tapi tidak semua, mungkin hash.

Deskripsi

Avast Mobile Security dengan antivirus gratis agar Android aman dari phishing, malware, spyware, dan virus berbahaya, seperti trojan… dan bahkan dari kehilangan atau pencurian. Amankan ponsel dan tablet Anda dengan aplikasi keamanan ponsel peringkat teratas kami secara gratis dengan perlindungan antivirus dan anti-pencurian.

✓ Alat pengaman seperti pemindai virus, pembersih/penghilang virus, pengukur jaringan, manajer aplikasi, penguncian aplikasi, dan bahkan firewall (pada ponsel yang sudah di-root) mengontrol sepenuhnya untuk tetap bersih.

✓ Melindungi dari infeksi umum dan ancaman berbasis WiFi terhadap OS kerentanan aplikasi.

✓ Temukan ponsel atau tablet yang hilang melalui fitur temukan ponsel berbasis web kami.

✓ Fitur penguncian jarak jauh dan penghapusan memori (hanya dua dari sekian banyak di komponen Anti-Pencurian lanjutannya) selalu mengamankan data Anda dari pencurian.

Ini benar-benar GRATIS.

Direkomendasikan oleh Android Authority terkemuka:

■ Android Authority: “Antivirus terbaik semakin baik… tidak ada yang sebaik ini.”
■ Android and Me: “Solusi anti-pencurian terbaik di pasaran.”
■ Android Police: “Apa pun yang Anda inginkan jika perangkat Anda hilang atau dicuri.”

MOBILE SECURITY | ANTIVIRUS UNTUK ANDROID

■ Antivirus Engine: Pemindai virus memindai aplikasi yang diinstal, konten kartu memori, dan aplikasi baru secara otomatis setelah digunakan pertama kali. Jadwal pemindaian otomatis saat Anda sedang tidur. Termasuk pemindaian SMS/file, untuk perlindungan ponsel sepenuhnya.

■ Laporan Privasi & Manajer Aplikasi: Dapatkan wawasan tentang aplikasi yang diinstal dan pahami hak-hak akses aplikasi, tujuan, dan perizinan Anda.

■ Filter SMS dan Panggilan: Menjaga privasi Anda. Blokir nomor-nomor yang tidak Anda inginkan untuk menghubungi Anda.

■ Proteksi Web: Blokir tautan yang terinfeksi malware, serta trojan, adware, dan spyware (untuk menjelajahi web dengan aman) dan bahkan nomor USSD (yang dapat menghapus memori perangkat Anda). Juga memperbaiki kesalahan pengetikan URL.

■ Penguncian Aplikasi: Kunci dua aplikasi mana pun dengan PIN/gerakan (tak terbatas dalam Premium).

■ Pencadangan: Mengizinkan pencadangan kontak, catatan SMS/panggilan, dan foto (Versi Premium menyediakan pencadangan musik, video, dan aplikasi).

TEMUKAN PONSEL SAYA | ANTI-PENCURIAN UNTUK ANDROID

■ Pelacak ponsel gratis terbaik di pasaran. Jika Anda berpikir “Bagaimana bisa saya menemukan Android saya?” Anda dapat menggunakan fitur penentu lokasi yang ada di ponsel untuk menemukannya, mengontrolnya dari jarak jauh, dan masih banyak.

■ Kontrol Android Anda dari jarak jauh melalui antarmuka berbasis web atau SMS (untuk mengontrol perangkat Anda dari jarak jauh nanti, buka: http://my.avast.com).

■ Temukan ponsel Anda di peta dengan menggunakan pelacak GPS.

■ Kunci perangkat, aktifkan sirene, atau hapus memori agar data privasi Anda tetap aman.

■ Dapatkan notifikasi atas perubahan kartu SIM.

BARU! FITUR PREMIUM | PILIHAN BERBAYAR

★ Penguncian Aplikasi: Mengunci sejumlah aplikasi tanpa batas.
★ Detektor Iklan: Mendeteksi iklan dan memberikan rincian lengkap tentang sistem pelacakannya.
★ Pengecekan Kata Sandi: Secara otomatis mengunci setelah 3 kali percobaan untuk membuka kunci.
★ Pemagaran Geografis: Ponsel melakukan tindakan tertentu (misalnya mengunci, membunyikan sirene, mengirimkan lokasi) saat berada di luar jarak yang sudah ditetapkan (misalnya Anda pergi ke kafe dan mengaktifkannya dengan jarak 500m, sehingga jika seseorang mencuri ponsel Anda dan membawanya di luar jarak ini, fitur ini akan melakukan tindakan yang Anda tentukan).
★ Perolehan Data Jarak Jauh: Mendapatkan kembali data dari ponsel dari jarak jauh.
★ Fitur Pencadangan: Memungkinkan pencadangan video, audio, dan aplikasi (termasuk pengaturan dan data untuk telepon yang di-root, misalnya kemajuan permainan