216 - 250 (Insan)

216. Langkah pertama dalam serangan yang sukses terhadap suatu sistem adalah:

A. mengumpulkan informasi.

B. mendapatkan akses.

C. menolak layanan.

D. menghindari deteksi.

Pembahasan:

A. Serangan yang sukses dimulai dengan mengumpulkan informasi tentang sistem target. Ini dilakukan di awal sehingga penyerang dapat mengetahui sistem target dan potensi kerentanan yang bisa dieksploitasi dalam serangan.

B. Setelah penyerang menemukan kerentanan potensial melalui pengumpulan informasi, mereka biasanya akan mencoba untuk mendapatkan akses.

C. Penyerang biasanya melancarkan serangan denial of service sebagai salah satu langkah terakhir dalam serangan.

D. Ketika penyerang telah mendapatkan akses dan mungkin menginfeksi korban dengan rootkit, mereka akan menghapus log audit dan mengambil langkah lain untuk menyembunyikan jejak mereka.

CIA (Confidentiality, Integrity, Availability)

A5-216: Pada pertanyaan ini, langkah pertama dalam serangan yang berhasil adalah mengumpulkan informasi. Ini berkaitan dengan kebutuhan untuk memahami sistem target dan kerentanan potensial yang dapat dieksploitasi.

217. Metode mana yang paling baik untuk mengurangi risiko pengungkapan informasi rahasia melalui penggunaan situs jejaring sosial?

A. Memberikan pelatihan kesadaran keamanan

B. Memerlukan kebijakan penggunaan yang dapat diterima yang ditandatangani

C. Memantau penggunaan media sosial

D. Memblokir akses ke media sosial

Pembahasan:

A. Memberikan pelatihan kesadaran keamanan adalah metode terbaik untuk mengurangi risiko pengungkapan informasi rahasia di situs jejaring sosial. Penting untuk diingat bahwa pengguna dapat mengakses layanan ini melalui cara lain seperti ponsel dan komputer rumah; oleh karena itu, pelatihan kesadaran adalah yang paling penting.

B. Memerlukan kebijakan penggunaan yang dapat diterima yang ditandatangani bisa menjadi kontrol yang baik. Namun, jika pengguna tidak sadar akan risikonya, maka kebijakan ini mungkin tidak efektif.

C. Memantau penggunaan media sosial melalui penggunaan server proxy yang melacak situs web yang dikunjungi pengguna bukanlah kontrol yang efektif karena pengguna dapat mengakses layanan ini melalui cara lain seperti ponsel dan komputer rumah.

D. Memblokir penggunaan media sosial melalui kontrol jaringan bukanlah kontrol yang efektif karena pengguna dapat mengakses layanan ini melalui cara lain seperti ponsel dan komputer rumah.

Control Type

A5-217: Soal ini menggambarkan bagaimana melindungi informasi rahasia melalui pelatihan kesadaran keamanan, yang terkait dengan kontrol organisasi dan kontrol manusia.

218. Seorang auditor IS menemukan bahwa ruang konferensi memiliki port jaringan aktif. Mana yang akan mencegah penemuan ini dari menyebabkan kekhawatiran?

A. Jaringan perusahaan menggunakan sistem pencegahan intrusi.

B. Bagian jaringan ini diisolasi dari jaringan perusahaan.

C. Solusi single sign-on telah diterapkan di jaringan perusahaan.

D. Perangkat lunak antivirus ada untuk melindungi jaringan perusahaan.

Pembahasan:

A. Sistem pencegahan intrusi mungkin menghentikan serangan, tetapi lebih baik membatasi kemampuan mesin di ruang konferensi untuk mengakses jaringan perusahaan sama sekali.

B. Jika ruang konferensi memiliki akses ke jaringan perusahaan, pengguna yang tidak sah mungkin dapat menghubungkan ke jaringan perusahaan; oleh karena itu,

kedua jaringan harus diisolasi baik melalui firewall atau dengan dipisahkan secara fisik.

C. Solusi single sign-on digunakan untuk kontrol akses tetapi tetap akan meninggalkan risiko ketika orang yang tidak sah memiliki akses fisik ke jaringan perusahaan.

D. Perangkat lunak antivirus akan mengurangi dampak dari kemungkinan virus; namun, pengguna yang tidak sah masih dapat mengakses jaringan perusahaan, yang merupakan risiko terbesar.

Control Type

Alasan: A5-218 membahas tentang jenis kontrol (isolasi) yang dapat mencegah port jaringan aktif di ruang konferensi menimbulkan kekhawatiran dengan mengisolasinya dari jaringan perusahaan.

219. Ketika melakukan uji penetrasi terhadap sistem TI, organisasi harus paling khawatir tentang:

A. kerahasiaan laporan.

B. menemukan semua kelemahan pada sistem.

C. mengembalikan sistem ke keadaan semula.

D. mencatat perubahan yang dibuat pada sistem produksi.

Pembahasan:

A. Laporan uji penetrasi adalah dokumen sensitif karena mencantumkan kerentanan dari sistem target. Namun, persyaratan utama untuk tim uji penetrasi adalah mengembalikan sistem ke kondisi semula.

B. Menemukan semua kemungkinan kelemahan tidak mungkin pada sistem informasi yang kompleks.

C. Setelah tes selesai, sistem harus dikembalikan ke keadaan semula. Dalam melakukan tes, perubahan mungkin telah dibuat pada aturan firewall, ID pengguna dibuat, atau file palsu diunggah. Semua ini harus dibersihkan sebelum tes selesai.

D. Semua perubahan yang dibuat harus dicatat, tetapi perhatian utama adalah memastikan bahwa perubahan tersebut dibalik pada akhir tes.

Control Type

A5-219: Pertanyaan ini menyoroti perlunya mengembalikan sistem ke keadaan aslinya setelah melakukan uji penetrasi, yang terkait dengan kontrol teknologi dan kontrol fisik dalam mengelola perubahan pada sistem.

220. Seorang auditor IS sedang meninjau sistem entri pesanan berbasis web yang baru seminggu sebelum sistem tersebut diluncurkan. Auditor IS telah mengidentifikasi bahwa aplikasi, seperti yang dirancang, mungkin kehilangan beberapa kontrol kritis mengenai bagaimana sistem menyimpan informasi kartu kredit pelanggan. Auditor IS harus terlebih dahulu:

A. menentukan apakah pengembang sistem memiliki pelatihan yang tepat tentang langkah-langkah keamanan yang memadai.

B. menentukan apakah administrator sistem telah menonaktifkan kontrol keamanan untuk alasan apapun.

C. memverifikasi bahwa persyaratan keamanan telah ditentukan dengan benar dalam rencana proyek.

D. memvalidasi apakah kontrol keamanan didasarkan pada persyaratan yang tidak lagi valid.

Pembahasan:

A. Meskipun penting bagi pemrogram untuk memahami keamanan, lebih penting bahwa persyaratan keamanan dinyatakan dengan benar dalam rencana proyek.

B. Administrator sistem mungkin telah membuat perubahan pada kontrol, tetapi diasumsikan bahwa auditor sedang meninjau sistem sebagaimana dirancang seminggu sebelum implementasi sehingga administrator belum mengkonfigurasi sistem.

C. Jika ada masalah keamanan signifikan yang diidentifikasi oleh auditor IS, pertanyaan pertama adalah apakah persyaratan keamanan sudah benar dalam rencana proyek. Tergantung pada apakah persyaratan tersebut termasuk dalam rencana akan mempengaruhi rekomendasi yang akan dibuat oleh auditor.

D. Mungkin persyaratan keamanan berubah dari waktu ke waktu berdasarkan ancaman atau kerentanan baru, tetapi jika kontrol kritis hilang, ini menunjuk pada desain yang salah yang didasarkan pada persyaratan yang tidak lengkap.

IS Framework & Standard (seperti ISO 27001, NIST)

A5-220: Pertanyaan ini menyoroti pentingnya memastikan bahwa persyaratan keamanan telah dinyatakan dengan benar dalam rencana proyek, yang terkait dengan kebutuhan untuk mematuhi standar dan kerangka kerja seperti ISO 27001.

221. Ketika melindungi sistem TI suatu organisasi, mana dari berikut ini yang biasanya menjadi lini pertahanan berikutnya setelah firewall jaringan telah dikompromikan?

A. Firewall pribadi

B. Program antivirus

C. Sistem deteksi intrusi

D. Konfigurasi virtual local area network (VLAN)

Pembahasan:

A. Firewall pribadi akan berada kemudian dalam strategi pertahanan, terletak di titik akhir.

B. Program antivirus akan diinstal pada titik akhir serta di jaringan, tetapi lapisan pertahanan berikutnya setelah firewall adalah sistem deteksi intrusi (IDS) atau sistem pencegahan intrusi (IPS).

C. IDS akan menjadi lini pertahanan berikutnya setelah firewall. IDS akan mendeteksi anomali dalam aktivitas jaringan/server dan mencoba mendeteksi pelakunya.

D. Konfigurasi virtual local area network tidak dimaksudkan untuk mengkompensasi kompromi firewall. Mereka adalah praktik arsitektur yang baik.

Security Event Management

A5-221: Soal ini berfokus pada langkah pertahanan berikutnya setelah firewall jaringan dikompromikan, yang berhubungan dengan deteksi intrusi dalam manajemen peristiwa keamanan.

222. Kontrol mana yang paling baik untuk mengurangi risiko serangan pharming pada aplikasi perbankan internet?

A. Kebijakan pendaftaran pengguna dan kata sandi

B. Kesadaran keamanan pengguna

C. Penggunaan sistem deteksi/pencegahan intrusi

D. Pengerasan server domain name system (DNS)

Pembahasan:

A. Kebijakan pendaftaran pengguna dan kata sandi tidak dapat mengurangi serangan pharming karena tidak mencegah manipulasi catatan domain name system (DNS).

B. Kesadaran keamanan pengguna tidak dapat mengurangi serangan pharming karena tidak mencegah manipulasi catatan DNS.

C. Penggunaan sistem pencegahan intrusi tidak dapat mengurangi serangan pharming karena mereka tidak mencegah manipulasi catatan DNS.

D. Serangan pharming mengalihkan lalu lintas ke situs web yang tidak sah dengan mengeksploitasi kerentanan pada server DNS. Untuk menghindari serangan semacam ini, perlu untuk menghilangkan kerentanan yang dapat memungkinkan peracunan DNS. Versi lama perangkat lunak DNS rentan terhadap serangan semacam ini dan harus ditambal.

Info Asset Security & Control

A5-222: Soal ini menyoroti kontrol terbaik untuk mengurangi risiko serangan pharming terhadap aplikasi perbankan internet, yang berkaitan dengan perlindungan privasi dan kontrol akses.

223. Mana dari berikut ini yang paling efektif meningkatkan keamanan sistem otentikasi berbasis tantangan-respons?

A. Memilih algoritma yang lebih kuat untuk menghasilkan string tantangan

B. Menerapkan langkah-langkah untuk mencegah serangan pembajakan sesi

C. Meningkatkan frekuensi perubahan kata sandi terkait

D. Meningkatkan panjang string otentikasi

Pembahasan:

A. Memilih algoritma yang lebih kuat akan meningkatkan keamanan; namun, ini mungkin tidak sepenting mitigasi risiko ketika dibandingkan dengan serangan man-in-the-middle.

B. Otentikasi berbasis tantangan-respons rentan terhadap serangan pembajakan sesi atau man-in-the-middle. Manajemen keamanan harus menyadari hal ini dan

melakukan penilaian risiko serta desain kontrol seperti otentikasi periodik saat menggunakan teknologi ini.

C. Sering mengubah kata sandi adalah praktik keamanan yang baik; namun, eksposur yang mengintai di jalur komunikasi mungkin menimbulkan risiko lebih besar.

D. Meningkatkan panjang string otentikasi tidak akan mencegah serangan man-in-the-middle atau pembajakan sesi.

Info Asset Security & Control

AS-223: Pertanyaan ini menyoroti peningkatan keamanan sistem autentikasi berbasis tantangan-respons, yang berkaitan dengan kontrol enkripsi dan kontrol akses.

224. Saat mengirim instruksi pembayaran, mana dari berikut ini yang akan membantu memverifikasi bahwa instruksi tersebut tidak diduplikasi?

A. Menggunakan algoritma hashing kriptografis

B. Mengenkripsi ringkasan pesan

C. Menghitung checksum transaksi

D. Menggunakan nomor urut dan stempel waktu

Pembahasan:

A. Penggunaan algoritma hashing kriptografis terhadap seluruh pesan membantu mencapai integritas data tetapi tidak akan mencegah pemrosesan duplikat.

B. Mengenkripsi ringkasan pesan menggunakan kunci pribadi pengirim, yang menandatangani tanda tangan digital pengirim pada dokumen, membantu dalam mengotentikasi sumber dan integritas transaksi tetapi tidak akan mencegah pemrosesan duplikat.

C. Checksum dapat digunakan untuk integritas data tetapi tidak untuk mencegah transaksi duplikat.

D. Saat mengirim data, nomor urut dan/atau stempel waktu yang dibangun ke dalam pesan untuk membuatnya unik dapat diperiksa oleh penerima untuk memastikan bahwa pesan tersebut tidak dicegat dan diputar ulang. Ini dikenal sebagai perlindungan replay dan dapat digunakan untuk memverifikasi bahwa instruksi pembayaran tidak diduplikasi.

Info Asset Security & Control

Relevan dengan sub-bab ini karena membahas perlindungan informasi sensitif, termasuk dalam konteks transmisi. Ini termasuk bagaimana mengelola risiko keamanan terkait dengan instruksi pembayaran, termasuk bagaimana mengkonfirmasi bahwa instruksi tersebut tidak diduplikasi.

225. Dalam komunikasi nirkabel, mana dari berikut ini yang memungkinkan perangkat penerima memverifikasi bahwa komunikasi yang diterima tidak diubah selama pengiriman?

A. Autentikasi perangkat dan autentikasi asal data

B. Sistem deteksi intrusi nirkabel dan sistem pencegahan intrusi

C. Penggunaan hashing kriptografis

D. Header dan trailer paket

Pembahasan:

A. Autentikasi perangkat dan autentikasi asal data memungkinkan titik akhir nirkabel untuk mengotentikasi satu sama lain untuk mencegah serangan man-in-the-middle dan penyamaran.

B. Sistem deteksi intrusi nirkabel dan sistem pencegahan intrusi memiliki kemampuan untuk mendeteksi perangkat yang salah konfigurasi dan perangkat jahat serta mendeteksi dan mungkin menghentikan jenis serangan tertentu.

C. Menghitung hashing kriptografis untuk komunikasi nirkabel memungkinkan perangkat penerima memverifikasi bahwa komunikasi yang diterima tidak diubah selama pengiriman. Ini mencegah penyamaran dan serangan modifikasi pesan.

D. Header dan trailer paket saja tidak memastikan bahwa konten tidak diubah karena seorang penyerang dapat mengubah baik data maupun trailer.

Info asset security & control

A5-225 menyoroti hash kriptografi untuk memverifikasi integritas data dalam komunikasi nirkabel.

226. Sebuah organisasi berencana untuk menggantikan jaringan kabel dengan jaringan nirkabel. Mana dari berikut ini yang PALING membantu mengamankan jaringan nirkabel dari akses yang tidak sah?

A. Mengimplementasikan Wired Equivalent Privacy.

B. Mengizinkan akses hanya untuk alamat kontrol akses media yang sah.

C. Menonaktifkan penyiaran terbuka dari service set identifiers.

D. Mengimplementasikan Wi-Fi Protected Access 2.

Pembahasan:

A. Wired Equivalent Privacy (WEP) dapat dibobol dalam hitungan menit. WEP menggunakan kunci statis yang harus dikomunikasikan kepada semua pengguna yang sah, sehingga manajemen menjadi sulit. Selain itu, ada kerentanan yang lebih besar jika kunci statis tidak diubah secara berkala.

B. Praktik mengizinkan akses berdasarkan alamat kontrol akses media (MAC) bukanlah solusi karena alamat MAC dapat dipalsukan oleh penyerang untuk mendapatkan akses ke jaringan.

C. Menonaktifkan penyiaran terbuka dari service set identifiers (SSID) tidak efektif sebagai kontrol akses karena banyak alat yang dapat mendeteksi titik akses nirkabel yang tidak menyebar.

D. Wi-Fi Protected Access 2 (WPA2) mengimplementasikan sebagian besar persyaratan standar IEEE 802.11i. Advanced Encryption Standard (AES) yang digunakan dalam WPA2 menyediakan keamanan yang lebih baik. Selain itu, WPA2 mendukung baik Extensible Authentication Protocol (EAP) maupun model autentikasi kunci pra-bagi (pre-shared key).

Info Asset Security & Control

A5-226: Pertanyaan ini berkaitan dengan pengamanan jaringan nirkabel dari akses yang tidak sah. Opsi jawaban berfokus pada langkah-langkah kontrol yang berkaitan dengan penggunaan jaringan nirkabel dan enkripsi, sehingga termasuk dalam domain Info Asset Security & Control.

227. Seorang auditor sistem informasi sedang meninjau konfigurasi firewall berbasis perangkat lunak. Mana dari berikut ini yang mewakili kerentanan TERBESAR?

A. Aturan implicit deny sebagai aturan terakhir dalam basis aturan.

B. Instalasi pada sistem operasi yang dikonfigurasi dengan pengaturan default.

C. Aturan yang mengizinkan atau menolak akses ke sistem atau jaringan.

D. Konfigurasi sebagai titik akhir jaringan pribadi virtual (VPN).

Pembahasan:

A. Mengkonfigurasi firewall dengan aturan implicit deny adalah praktik umum.

B. Pengaturan default dari sebagian besar peralatan, termasuk sistem operasi, sering dipublikasikan dan memberikan informasi konfigurasi yang dapat diprediksi kepada penyusup, yang memungkinkan kompromi sistem lebih mudah. Untuk mengurangi risiko ini, perangkat lunak firewall harus diinstal pada sistem yang menggunakan sistem operasi yang diperkuat yang memiliki fungsionalitas terbatas, menyediakan hanya layanan yang diperlukan untuk mendukung perangkat lunak firewall.

C. Konfigurasi firewall harus memiliki aturan yang mengizinkan atau menolak akses sesuai dengan kebijakan.

D. Firewall sering dikonfigurasikan sebagai titik akhir untuk VPN.

Control Type

A5-227: Soal ini membahas kerentanan terbesar dalam konfigurasi firewall berbasis perangkat lunak. Opsi jawaban menyoroti berbagai konfigurasi yang relevan dengan kontrol yang terkait dengan jenis kontrol yang diterapkan dalam sebuah firewall, yang merupakan bagian dari Control Type.

228. Risiko TERBESAR dari sistem pencegahan intrusi yang diimplementasikan dengan tidak benar adalah:

A. Terlalu banyak peringatan untuk diverifikasi oleh administrator sistem.

B. Penurunan kinerja jaringan karena lalu lintas tambahan.

C. Pemblokiran sistem atau layanan kritis karena pemicu palsu.

D. Ketergantungan pada keahlian khusus dalam organisasi TI.

Pembahasan:

A. Sejumlah positif palsu dapat menyebabkan beban kerja administrator yang berlebihan tetapi ini adalah risiko yang relatif kecil.

B. Sistem pencegahan intrusi tidak akan menghasilkan lalu lintas yang akan mempengaruhi kinerja jaringan.

C. Sistem pencegahan intrusi (IPS) mencegah koneksi atau layanan berdasarkan bagaimana ia diprogram untuk bereaksi terhadap insiden tertentu. Jika IPS dipicu berdasarkan perilaku yang didefinisikan secara tidak benar atau tidak standar, ia dapat memblokir layanan atau koneksi dari sistem internal yang kritis.

D. Mengonfigurasi IPS dapat memakan waktu berbulan-bulan untuk mempelajari apa yang dapat diterima dan apa yang tidak, tetapi ini tidak memerlukan keahlian khusus.

Security Event Management (Visibility, Detection, Response)

A5-228: Membahas risiko terbesar dari Intrusion Prevention System (IPS) yang diimplementasikan secara tidak tepat (pemblokiran layanan kritis)- Detection

229. Ketika meninjau proses verifikasi sertifikat digital, mana dari temuan berikut yang mewakili risiko PALING signifikan?

A. Tidak ada otoritas pendaftaran untuk melaporkan kompromi kunci.

B. Daftar pencabutan sertifikat tidak terbaru.

C. Sertifikat digital mengandung kunci publik yang digunakan untuk mengenkripsi pesan dan memverifikasi tanda tangan digital.

D. Pelanggan melaporkan kompromi kunci kepada otoritas sertifikat.

Pembahasan:

A. Otoritas sertifikat (CA) dapat mengambil alih tanggung jawab jika tidak ada otoritas pendaftaran (RA).

B. Jika daftar pencabutan sertifikat (CRL) tidak terbaru, mungkin ada sertifikat digital yang tidak dicabut yang dapat digunakan untuk aktivitas yang tidak sah atau penipuan.

C. Sertifikat digital mengandung kunci publik yang digunakan untuk mengenkripsi pesan dan memverifikasi tanda tangan digital; oleh karena itu, ini bukan risiko.

D. Pelanggan melaporkan kompromi kunci kepada CA bukanlah risiko karena melaporkan ini kepada CA memungkinkan CA untuk mengambil tindakan yang sesuai.

Info Asset Security & Control

karena fokusnya pada temuan terkait daftar pencabutan sertifikat digital yang tidak terbaru dalam proses verifikasi sertifikat digital.

230. Saat menggunakan tanda tangan digital, ringkasan pesan dihitung oleh:

A. hanya pengirim.

B. hanya penerima.

C. pengirim dan penerima keduanya.

D. otoritas sertifikat.

Pembahasan:

A. Ringkasan pesan harus dihitung oleh pengirim dan penerima untuk memastikan integritas pesan.

B. Penerima akan menghitung ulang ringkasan pesan yang diterima untuk memverifikasi integritas pesan yang diterima.

C. Tanda tangan digital adalah identifikasi elektronik dari seseorang atau entitas. Ini dibuat dengan menggunakan enkripsi asimetris. Untuk memverifikasi integritas data, pengirim menggunakan algoritma hashing kriptografi terhadap seluruh pesan untuk membuat ringkasan pesan yang akan dikirim bersama dengan pesan. Setelah menerima pesan, penerima akan menghitung ulang hash menggunakan algoritma yang sama.

D. Otoritas sertifikat (CA) mengeluarkan sertifikat yang menghubungkan kunci publik dengan pemiliknya. CA tidak menghitung ringkasan pesan yang akan dikomunikasikan antara pengirim dan penerima.

Info Asset Security & Control

karena fokusnya pada perhitungan message digest dalam tanda tangan digital, yang merupakan komponen penting dalam memastikan integritas dan keaslian pesan.

231. Mana dari berikut ini yang secara efektif memverifikasi asal pengirim transaksi?

A. Menggunakan kata sandi rahasia antara pengirim dan penerima.

B. Mengenkripsi transaksi dengan kunci publik penerima.

C. Menggunakan format dokumen portabel untuk mengenkapsulasi konten transaksi.

D. Menandatangani transaksi secara digital dengan kunci pribadi sumber.

Pembahasan:

A. Karena kata sandi adalah "rahasia bersama" antara pengguna dan sistem itu sendiri, kata sandi dianggap sebagai cara autentikasi yang lebih lemah.

B. Mengenkripsi transaksi dengan kunci publik penerima akan memberikan kerahasiaan untuk informasi tetapi tidak akan memverifikasi sumbernya.

C. Menggunakan format dokumen portabel akan melindungi integritas konten tetapi tidak serta-merta memastikan kepenulisan.

D. Tanda tangan digital adalah identifikasi elektronik seseorang, yang dibuat dengan menggunakan algoritma kunci publik, untuk memverifikasi identitas sumber transaksi dan integritas kontennya kepada penerima.

Info Asset Security & Control

karena fokusnya pada jenis autentikasi yang paling aman untuk aplikasi web. Autentikasi yang aman sangat penting untuk melindungi data sensitif pengguna dalam aplikasi web.

232. Sebuah organisasi telah membangun jaringan tamu untuk akses pengunjung. Mana dari berikut ini yang harus menjadi perhatian TERBESAR seorang auditor sistem informasi?

A. Layar login tidak ditampilkan untuk pengguna tamu.

B. Jaringan tamu tidak dipisahkan dari jaringan produksi.

C. Pengguna tamu yang login tidak diisolasi satu sama lain.

D. Teknik autentikasi satu faktor digunakan untuk memberikan akses.

Pembahasan:

A. Menggunakan portal web captive, yang menampilkan layar login di browser web pengguna, adalah praktik yang baik untuk mengautentikasi tamu. Namun, jika jaringan

tamu tidak dipisahkan dari jaringan produksi, pengguna dapat memperkenalkan malware dan berpotensi mendapatkan akses yang tidak pantas ke sistem dan informasi.

B. Implikasinya adalah tamu memiliki akses ke jaringan organisasi. Mengizinkan pengguna yang tidak dipercaya untuk terhubung ke jaringan organisasi dapat memperkenalkan malware dan berpotensi memungkinkan individu-individu ini mendapatkan akses yang tidak pantas ke sistem dan informasi.

C. Ada platform tertentu di mana diizinkan bagi tamu untuk berinteraksi satu sama lain. Selain itu, tamu dapat diperingatkan untuk hanya menggunakan sistem yang aman dan kebijakan yang mencakup interaksi antara tamu dapat dibuat.

D. Meskipun teknik autentikasi multifaktor lebih disukai, metode autentikasi satu faktor harus memadai jika diimplementasikan dengan benar.

Control Type

karena fokusnya pada segregasi jaringan, yang merupakan jenis kontrol fisik yang digunakan untuk meningkatkan keamanan jaringan.

233. Yang memberikan jaminan TERBESAR untuk enkripsi kata sandi basis data adalah:

A. Secure hash algorithm-256

B. Advanced encryption standard

C. Secure Shell

D. Triple data encryption standard

Pembahasan:

A. Fungsi hashing sering digunakan untuk melindungi kata sandi, tetapi hashing bukanlah enkripsi.

B. Penggunaan advanced encryption standard (AES) adalah algoritma enkripsi yang aman yang cocok untuk mengenkripsi kata sandi.

C. Secure Shell dapat mengenkripsi kata sandi yang sedang dikirim tetapi tidak mengenkripsi data yang disimpan.

D. Triple Data Encryption Standard adalah metode enkripsi yang valid; namun, AES adalah algoritma enkripsi yang lebih kuat dan lebih baru.

Control Type

karena fokusnya pada pengujian penetrasi, yang merupakan jenis kontrol teknologi yang digunakan untuk mengidentifikasi kerentanan keamanan dalam sistem informasi.

234. Alasan proses sertifikasi dan akreditasi dilakukan pada sistem kritis adalah untuk memastikan bahwa:

A. Kepatuhan keamanan telah dievaluasi secara teknis.

B. Data telah dienkripsi dan siap untuk disimpan.

C. Sistem telah diuji untuk dijalankan pada berbagai platform.

D. Sistem telah mengikuti fase model air terjun.

Pembahasan:

A. Sistem yang telah disertifikasi dan diakreditasi adalah sistem yang telah dievaluasi kepatuhan keamanannya untuk dijalankan di lingkungan dan konfigurasi tertentu.

B. Pengujian sertifikasi mencakup fungsionalitas keamanan, termasuk enkripsi jika diperlukan, tetapi itu bukan tujuan utama dari proses sertifikasi dan akreditasi (C&A).

C. Sistem yang disertifikasi dievaluasi untuk dijalankan di lingkungan tertentu.

D. Model air terjun adalah metodologi pengembangan perangkat lunak dan bukan alasan untuk melakukan proses C&A.

IS framework standard – PDCA - Check

karena fokusnya pada logging dan monitoring, yang merupakan bagian penting dari operasi keamanan yang membantu organisasi untuk mendeteksi aktivitas mencurigakan, mematuhi peraturan, dan meningkatkan keamanan.

235. Seorang pelaku yang ingin mendapatkan akses dan mengumpulkan informasi tentang data terenkripsi yang dikirimkan melalui jaringan kemungkinan besar akan menggunakan:

A. penyadapan.

B. spoofing.

C. analisis lalu lintas.

D. menyamar.

Pembahasan:

A. Dalam penyadapan, yang merupakan serangan pasif, pelaku mengumpulkan informasi yang mengalir melalui jaringan dengan tujuan memperoleh konten pesan untuk analisis pribadi atau untuk pihak ketiga. Lalu lintas terenkripsi umumnya dilindungi dari penyadapan.

B. Spoofing adalah serangan aktif. Dalam spoofing, pengguna menerima email yang tampaknya berasal dari satu sumber padahal sebenarnya dikirim dari sumber lain.

C. Dalam analisis lalu lintas, yang merupakan serangan pasif, pelaku menentukan sifat aliran lalu lintas antara host yang ditentukan dan melalui analisis panjang sesi, frekuensi, dan panjang pesan, pelaku dapat menebak jenis komunikasi yang sedang terjadi. Ini biasanya digunakan saat pesan terenkripsi, dan penyadapan tidak akan menghasilkan hasil yang berarti.

D. Dalam menyamar, pelaku menyajikan identitas selain identitas aslinya. Ini adalah serangan aktif.

Security Event Management (Visibility, Detection, Response)

A5-235: Menjelaskan risiko analisis lalu lintas untuk data terenkripsi (serangan pasif) - Visibilitas.

236. Sebuah hotel telah menempatkan PC di lobi untuk menyediakan akses internet bagi tamu. Manakah dari berikut ini yang merupakan risiko TERBESAR untuk pencurian identitas?

A. Cookie browser web tidak dihapus secara otomatis.

B. Komputer dikonfigurasi dengan tidak benar.

C. Pembaruan sistem tidak diterapkan pada komputer.

D. Timeout sesi tidak diaktifkan.

Pembahasan:

A. Jika cookie browser web tidak dihapus secara otomatis, mungkin saja untuk menentukan situs web yang diakses pengguna. Namun, jika sesi tidak habis waktu, lebih mudah untuk terjadi pencurian identitas.

B. Jika PC tidak dikonfigurasi dengan benar dan tidak memiliki perangkat lunak antivirus yang terpasang, mungkin ada risiko infeksi virus atau malware. Ini bisa menyebabkan

pencurian identitas. Namun, jika sesi tidak habis waktu, lebih mudah untuk terjadi pencurian identitas.

C. Jika pembaruan sistem tidak diterapkan, mungkin ada risiko infeksi virus atau malware yang lebih besar. Ini bisa menyebabkan pencurian identitas. Namun, jika sesi tidak habis waktu, lebih mudah untuk terjadi pencurian identitas.

D. Jika sesi yang diautentikasi tidak aktif dan tidak diawasi, sesi tersebut dapat dibajak dan digunakan untuk tujuan ilegal. Akan sulit untuk menentukan pelaku karena sesi yang sah digunakan.

Control Type

A5-236: Pertanyaan ini berkaitan dengan risiko terbesar terkait sistem kontrol akses fisik. Opsi jawaban menyoroti kontrol akses fisik yang berhubungan dengan penggunaan kartu akses, sehingga relevan dengan Control Type.

237. Sistem kontrol biometrik yang PALING efektif adalah yang memiliki:

A. tingkat kesalahan sama tertinggi.

B. tingkat kesalahan sama terendah.

C. tingkat penolakan palsu sama dengan tingkat penerimaan palsu.

D. tingkat penolakan palsu sama dengan tingkat kegagalan mendaftar.

Pembahasan:

A. Biometrik yang memiliki tingkat kesalahan sama (EER) tertinggi adalah yang paling tidak efektif.

B. EER dari sistem biometrik menunjukkan persentase di mana tingkat penerimaan palsu (FAR) sama dengan tingkat penolakan palsu (FRR). Biometrik yang memiliki EER terendah adalah yang paling efektif.

C. Untuk setiap biometrik, akan ada ukuran di mana FRR akan sama dengan FAR. Ini adalah EER.

D. Tingkat kegagalan mendaftar (FER) adalah ukuran agregat dari FRR.

Control Type

karena fokusnya pada sistem kontrol biometrik, yang merupakan jenis kontrol teknologi yang digunakan untuk melakukan autentikasi.

238. Manakah dari berikut ini yang merupakan bentuk autentikasi pengguna dua faktor?

A. Kartu pintar dan nomor identifikasi pribadi.

B. ID pengguna unik dan kata sandi kompleks, bukan dari kamus.

C. Pindai iris dan pindai sidik jari.

D. Kartu pita magnetik dan lencana kedekatan.

Pembahasan:

A. Kartu pintar adalah sesuatu yang dimiliki pengguna, sementara nomor identifikasi pribadi yang dipasangkan dengan kartu adalah sesuatu yang diketahui pengguna. Ini adalah contoh autentikasi dua faktor.

B. Baik ID dan kata sandi adalah sesuatu yang diketahui pengguna, jadi ini adalah autentikasi pengguna satu faktor terlepas dari kompleksitasnya.

C. Baik pindai iris dan pindai sidik jari adalah sesuatu yang dimiliki pengguna, jadi ini bukan basis untuk autentikasi pengguna dua faktor.

D. Baik kartu magnetik dan lencana kedekatan adalah contoh sesuatu yang dimiliki pengguna, jadi ini tidak memadai untuk autentikasi dua faktor.

Info Asset Security & Control

A5-238: Pertanyaan ini berkaitan dengan otentikasi pengguna dua faktor. Jawaban yang benar menyoroti penggunaan kartu pintar dan PIN, yang merupakan metode otentikasi yang sering kali diterapkan dalam Info Asset Security & Control.

239. Seorang auditor IS sedang meninjau langkah-langkah keamanan fisik sebuah organisasi. Mengenai sistem kartu akses, auditor IS harus PALING khawatir bahwa:

A. Kartu akses non-personal diberikan kepada staf kebersihan, yang menggunakan lembar masuk tetapi tidak menunjukkan bukti identitas.

B. Kartu akses tidak diberi label dengan nama dan alamat organisasi untuk memudahkan pengembalian jika hilang.

C. Penerbitan kartu dan administrasi hak kartu dilakukan oleh departemen yang berbeda, menyebabkan waktu tunggu yang tidak perlu untuk kartu baru.

D. Sistem komputer yang digunakan untuk memprogram kartu hanya dapat diganti setelah tiga minggu jika terjadi kegagalan sistem.

Pembahasan:

A. Keamanan fisik dimaksudkan untuk mengontrol siapa yang memasuki area yang aman, jadi identifikasi semua individu sangat penting. Tidak cukup mempercayai orang luar yang tidak dikenal dengan membiarkan mereka menulis nama mereka tanpa bukti (misalnya, kartu identitas, SIM).

B. Menampilkan nama dan alamat organisasi pada kartu mungkin menjadi kekhawatiran karena seseorang yang jahat bisa menggunakan kartu yang hilang atau dicuri untuk memasuki tempat organisasi.

C. Memisahkan penerbitan kartu dari manajemen hak teknis adalah metode untuk memastikan pemisahan tugas yang tepat sehingga tidak ada satu orang pun yang dapat memproduksi kartu yang berfungsi untuk area yang dibatasi dalam tempat organisasi. Waktu tunggu yang lama adalah ketidaknyamanan tetapi bukan risiko audit yang serius.

D. Kegagalan sistem perangkat pemrograman kartu biasanya tidak berarti pembaca tidak berfungsi lagi. Ini hanya berarti tidak ada kartu baru yang dapat diterbitkan, jadi opsi ini lebih ringan dibandingkan dengan ancaman identifikasi yang tidak tepat.

Control Type

A5-239: Soal ini menyoroti kekhawatiran terbesar terkait sistem kartu akses. Opsi jawaban menyoroti kontrol akses fisik yang berhubungan dengan manajemen kartu akses-kontrol fisik

A5-240

Ketika meninjau prosedur untuk pembuangan komputer, mana dari berikut ini yang harus menjadi kekhawatiran TERBESAR bagi auditor IS?

A. Hard disk dihapus beberapa kali pada tingkat sektor tetapi tidak diformat ulang sebelum meninggalkan organisasi.

B. Semua file dan folder di hard disk dihapus secara terpisah dan hard disk diformat sebelum meninggalkan organisasi.

C. Hard disk dirusak dengan membuat lubang pada platter di posisi tertentu sebelum meninggalkan organisasi.

D. Transportasi hard disk dikawal oleh staf keamanan internal ke perusahaan daur ulang logam terdekat, di mana hard disk didaftarkan dan kemudian dihancurkan.

Pembahasan:

A. Menimpa hard disk pada tingkat sektor akan sepenuhnya menghapus data, direktori, indeks, dan tabel file utama. Memformat ulang tidak diperlukan karena semua konten dihancurkan. Menimpa beberapa kali membuat beberapa langkah forensik tidak berguna, yang dapat merekonstruksi konten sebelumnya dari sektor yang baru ditimpa dengan menganalisis fitur magnetik khusus dari permukaan platter.

B. Menghapus dan memformat hanya menandai sektor yang berisi file sebagai bebas. Alat yang tersedia untuk umum cukup untuk seseorang merekonstruksi data dari hard drive yang dipersiapkan dengan cara ini.

C. Meskipun membuat lubang tidak menghapus konten file, hard disk tidak dapat digunakan lagi, terutama ketika zona parkir kepala dan informasi track zero terpengaruh. Merekonstruksi data akan sangat mahal karena semua analisis harus dilakukan di bawah atmosfer ruang bersih dan hanya mungkin pada bagian kecil dari hard disk pada satu waktu. Ini adalah metode yang lebih ringan daripada opsi B.

D. Dengan penghancuran yang dilakukan di bawah pengawasan keamanan, hampir tidak ada peluang bahwa isi drive yang digunakan akan bocor.

Control Type

A5-240: Menjelaskan metode pembuangan hard disk yang paling aman (penghancuran) - Kontrol Fisik.

241. Sebuah aplikasi bisnis baru memerlukan penyimpangan dari konfigurasi standar sistem operasi (OS). Aktivitas apa yang seharusnya direkomendasikan oleh auditor IS kepada manajer keamanan sebagai tanggapan PERTAMA?

A. Penolakan awal terhadap permintaan karena bertentangan dengan kebijakan keamanan

B. Persetujuan pengecualian terhadap kebijakan untuk memenuhi kebutuhan bisnis

C. Penilaian risiko dan identifikasi pengendalian kompensasi

D. Revisi konfigurasi dasar OS

Pembahasan:

A. Kebijakan keamanan dapat dikecualikan dengan persetujuan manajemen untuk memenuhi persyaratan bisnis; bukan hak manajer keamanan untuk menolak penyimpangan.

B. Manajer keamanan mungkin dapat mengusulkan penyimpangan dari kebijakan, tetapi ini harus didasarkan pada penilaian risiko dan pengendalian kompensasi. Penyimpangan itu sendiri harus disetujui sesuai dengan proses penanganan pengecualian yang telah ditetapkan.

C. Sebelum menyetujui pengecualian apapun, manajer keamanan harus terlebih dahulu memeriksa pengendalian kompensasi dan menilai risiko yang mungkin timbul akibat penyimpangan tersebut.

D. Memperbarui atau merevisi konfigurasi dasar tidak terkait dengan permintaan untuk penyimpangan.

Control Type - Organizational Control

karena fokusnya pada penilaian risiko dan identifikasi kontrol kompensasi terkait deviasi dari konfigurasi standar sistem operasi.

242. Sebuah organisasi telah membuat kebijakan yang mendefinisikan jenis situs web yang dilarang diakses oleh pengguna. Teknologi apa yang PALING efektif untuk menegakkan kebijakan ini?

A. Stateful inspection firewall

B. Filter konten web

C. Server cache web

D. Server proxy

Pembahasan:

A. Stateful inspection firewall tidak banyak membantu dalam menyaring lalu lintas web karena tidak meninjau konten situs web, juga tidak memperhatikan klasifikasi situs tersebut.

B. Filter konten web menerima atau menolak komunikasi web sesuai dengan aturan yang dikonfigurasi. Untuk membantu administrator mengkonfigurasi alat ini

dengan benar, organisasi dan vendor telah menyediakan daftar hitam URL dan klasifikasi untuk jutaan situs web.

C. Server cache web dirancang untuk meningkatkan kecepatan pengambilan halaman web yang paling umum atau baru saja dikunjungi.

D. Server proxy adalah salah karena server proxy melayani permintaan kliennya dengan meneruskan permintaan ke server lain. Banyak orang secara keliru menggunakan server proxy sebagai sinonim dari server web proxy meskipun tidak semua server web proxy memiliki kemampuan penyaringan konten.

Control Type – tech control

Soal ini membahas tentang penggunaan web content filter, yang merupakan jenis kontrol teknologi yang digunakan untuk menegakkan kebijakan akses website.

243. Mana dari berikut ini yang secara khusus menangani cara mendeteksi serangan siber terhadap sistem TI organisasi dan cara memulihkan diri dari serangan?

A. Rencana tanggap insiden

B. Rencana kontingensi TI

C. Rencana keberlangsungan bisnis

D. Rencana kelangsungan operasi

Pembahasan:

A. Rencana tanggap insiden (IRP) menentukan tanggapan keamanan informasi terhadap insiden seperti serangan siber pada sistem dan/atau jaringan. Rencana ini menetapkan prosedur untuk memungkinkan personel keamanan mengidentifikasi, mengurangi, dan memulihkan dari insiden komputer berbahaya seperti akses tidak sah ke sistem atau data, penolakan layanan, atau perubahan tidak sah pada perangkat keras atau perangkat lunak sistem.

B. Rencana kontingensi TI menangani gangguan sistem TI dan menetapkan prosedur untuk memulihkan dari kegagalan aplikasi utama atau sistem pendukung umum. Rencana kontingensi menangani cara memulihkan dari kegagalan yang tidak terduga, tetapi tidak menangani identifikasi atau pencegahan serangan siber.

C. Rencana keberlangsungan bisnis (BCP) menangani proses bisnis dan menyediakan prosedur untuk mempertahankan operasi bisnis penting saat memulihkan dari gangguan yang signifikan. Sementara serangan siber bisa cukup parah untuk memerlukan penggunaan BCP, IRP akan digunakan untuk menentukan tindakan yang harus diambil – baik untuk menghentikan serangan maupun untuk melanjutkan operasi normal setelah serangan.

D. Rencana kelangsungan operasi menangani subset dari misi organisasi yang dianggap paling kritis dan berisi prosedur untuk mempertahankan fungsi-fungsi ini di situs alternatif untuk jangka waktu pendek.

Security event manegement

Soal ini membahas tentang rencana penanganan insiden (incident response plan) yang digunakan untuk mendeteksi serangan siber dan melakukan pemulihan.

244. Hasil hash kriptografis dari sebuah pesan dihitung ulang oleh penerima. Ini untuk memastikan:

A. kerahasiaan pesan.

B. nonrepudiation oleh pengirim.

C. keaslian pesan.

D. integritas data yang dikirim oleh pengirim.

Pembahasan:

A. Fungsi hash memastikan integritas pesan; enkripsi dengan kunci rahasia memberikan kerahasiaan.

B. Menandatangani pesan dengan kunci pribadi pengirim memastikan nonrepudiation dan keaslian.

C. Keaslian pesan diberikan oleh tanda tangan digital.

D. Jika hasil hash berbeda dari yang diharapkan, itu berarti bahwa pesan telah diubah. Ini adalah uji integritas.

Info Asset Security & Control

Kriptografi adalah salah satu teknik yang digunakan untuk menjaga keamanan informasi dengan memastikan kerahasiaan, integritas, dan autentikasi data.

245. Tim respons insiden keamanan komputer dari sebuah organisasi menyebarkan deskripsi rinci tentang ancaman terbaru. Kekhawatiran TERBESAR dari seorang auditor IS seharusnya adalah bahwa pengguna mungkin:

A. menggunakan informasi ini untuk meluncurkan serangan.

B. meneruskan peringatan keamanan.

C. menerapkan solusi individu.

D. gagal memahami ancaman.

Pembahasan:

A. Tim respons insiden keamanan komputer (CSIRT) dari sebuah organisasi harus menyebarkan ancaman terbaru, pedoman keamanan, dan pembaruan keamanan kepada pengguna untuk membantu mereka memahami risiko keamanan dari kesalahan dan kelalaian. Namun, ini memperkenalkan risiko bahwa pengguna mungkin menggunakan informasi ini untuk meluncurkan serangan, secara langsung atau tidak langsung. Seorang auditor IS harus memastikan bahwa CSIRT terlibat aktif dengan pengguna untuk membantu mereka dalam mitigasi risiko yang timbul dari kegagalan keamanan dan untuk mencegah insiden keamanan tambahan yang diakibatkan oleh ancaman yang sama.

B. Meneruskan peringatan keamanan tidak merugikan organisasi.

C. Menerapkan solusi individu tidak mungkin dan tidak efisien, tetapi bukan risiko serius.

D. Pengguna yang gagal memahami ancaman bukanlah kekhawatiran serius.

Security event management

Soal A5-245 berkaitan dengan tindakan yang dilakukan oleh tim respons insiden keamanan komputer dalam menyebarkan informasi tentang ancaman keamanan kepada pengguna. Ini berkaitan dengan manajemen kejadian keamanan, khususnya dalam hal deteksi serangan siber terhadap sistem TI organisasi dan bagaimana untuk pulih dari serangan tersebut.

A5-246

Indikator mana dari berikut ini yang menunjukkan efektivitas tim respons insiden keamanan komputer?

A. Dampak finansial per insiden keamanan

B. Jumlah kerentanan keamanan yang telah diperbaiki

C. Persentase aplikasi bisnis yang dilindungi

D. Jumlah tes penetrasi yang berhasil

Pembahasan:

A. Indikator paling penting adalah dampak finansial per insiden keamanan. Mungkin tidak mungkin untuk mencegah insiden sepenuhnya, tetapi tim harus dapat membatasi biaya insiden melalui kombinasi pencegahan, deteksi, dan respons yang efektif.

B. Memperbaiki kerentanan keamanan adalah penting tetapi bukan tanggung jawab langsung tim respons insiden keamanan komputer (CSIRT).

C. CSIRT tidak bertanggung jawab untuk perlindungan sistem. Itu adalah tanggung jawab tim keamanan.

D. Jumlah tes penetrasi mengukur efektivitas tim keamanan dan proses manajemen tambalan, tetapi bukan efektivitas CSIRT.

Security event management

Soal A5-246 berkaitan dengan pengukuran efektivitas dari tim respons insiden keamanan komputer. Ini menanyakan indikator yang paling tepat untuk menilai seberapa baik tim tersebut berkinerja. Hal ini terkait dengan manajemen kejadian keamanan

247. Manfaat dari kualitas layanan adalah bahwa:

A. ketersediaan dan kinerja seluruh jaringan akan sangat meningkat.

B. operator telekomunikasi akan memberikan laporan kepatuhan layanan yang akurat kepada perusahaan.

C. aplikasi yang berpartisipasi akan memiliki jaminan bandwidth.

D. tautan komunikasi akan didukung oleh kontrol keamanan untuk melakukan transaksi online yang aman.

Pembahasan:

A. Kualitas layanan (QoS) tidak menjamin bahwa komunikasi itu sendiri akan meningkat. Meskipun kecepatan pertukaran data untuk aplikasi tertentu bisa lebih cepat, ketersediaan tidak akan meningkat.

B. Alat QoS yang digunakan oleh banyak operator tidak menyediakan laporan tingkat layanan; namun, ada alat lain yang akan menghasilkan laporan tingkat layanan.

C. Fungsi utama QoS adalah mengoptimalkan kinerja jaringan dengan memberikan prioritas kepada aplikasi bisnis dan pengguna akhir melalui alokasi bagian tertentu dari bandwidth untuk lalu lintas tertentu.

D. Meskipun QoS diintegrasikan dengan firewall, jaringan pribadi virtual (VPN), alat enkripsi, dan lainnya, alat itu sendiri tidak dimaksudkan untuk menyediakan kontrol keamanan.

CIA

Soal A5-247 berkaitan dengan manfaat dari Quality of Service (QoS), yang merupakan bagian dari sub bab "Protection of Information Assets". QoS adalah konsep yang menjamin kualitas layanan jaringan dengan memberikan prioritas tertentu pada jenis lalu lintas data yang berbeda. Ini memastikan bahwa aplikasi yang lebih penting mendapatkan bandwidth yang cukup untuk beroperasi dengan baik. Jadi, soal ini terkait dengan aspek Availability (Ketersediaan) dari prinsip-prinsip CIA (Confidentiality, Integrity, Availability).

248. Prosedur mana dari berikut ini yang PALING efektif untuk mendeteksi pemuatan paket perangkat lunak ilegal ke dalam jaringan?

A. Penggunaan workstation tanpa disk

B. Pemeriksaan berkala terhadap hard drive

C. Penggunaan perangkat lunak antivirus terbaru

D. Kebijakan yang mengakibatkan pemecatan instan jika dilanggar

Pembahasan:

A. Workstation tanpa disk berfungsi sebagai kontrol pencegahan dan tidak sepenuhnya efektif dalam mencegah pengguna mengakses perangkat lunak ilegal melalui jaringan.

B. Pemeriksaan berkala terhadap hard drive adalah metode paling efektif untuk mengidentifikasi paket perangkat lunak ilegal yang dimuat ke dalam jaringan.

C. Perangkat lunak antivirus tidak akan selalu mengidentifikasi perangkat lunak ilegal, kecuali perangkat lunak tersebut mengandung virus.

D. Kebijakan adalah kontrol pencegahan yang menetapkan aturan tentang memuat perangkat lunak, tetapi tidak akan mendeteksi kejadian sebenarnya.

Security event management

Soal A5-248 berhubungan dengan cara yang paling efektif untuk mendeteksi pemasangan paket perangkat lunak ilegal ke dalam jaringan. Jawabannya adalah opsi B, yaitu "Periodic checking of hard drives" (Pemeriksaan berkala pada hard drive). Tindakan ini akan memungkinkan organisasi untuk secara rutin memeriksa isi hard drive untuk mendeteksi keberadaan perangkat lunak ilegal. Hal ini sesuai dengan prinsip-prinsip kontrol teknologi yang melibatkan pengawasan dan pemantauan terhadap sistem informasi untuk mencegah, mendeteksi, dan menanggapi insiden keamanan

249. Sebuah perusahaan perdagangan saham online sedang dalam proses mengimplementasikan sistem untuk menyediakan pertukaran email yang aman dengan pelanggannya. Opsi mana yang TERBAIK untuk memastikan kerahasiaan, integritas, dan nonrepudiation?

A. Enkripsi kunci simetris

B. Tanda tangan digital

C. Algoritma ringkasan pesan

D. Sertifikat digital

Pembahasan:

A. Enkripsi kunci simetris menggunakan satu kata sandi untuk mengenkripsi dan mendekripsi pesan. Meskipun jenis enkripsi ini kuat, ia memiliki masalah inheren dalam berbagi kata sandi dengan cara yang aman dan tidak menangani integritas dan nonrepudiation.

B. Tanda tangan digital menyediakan integritas pesan dan nonrepudiation; namun, kerahasiaan tidak disediakan.

C. Algoritma ringkasan pesan adalah cara untuk merancang fungsi hash untuk memverifikasi integritas pesan/data. Algoritma ringkasan pesan tidak menyediakan kerahasiaan atau nonrepudiation.

D. Sertifikat digital berisi kunci publik dan informasi identifikasi tentang pemilik kunci publik. Pasangan kunci pribadi yang terkait disimpan rahasia oleh pemilik. Sertifikat ini biasanya diverifikasi oleh otoritas tepercaya, dengan tujuan mengasosiasikan identitas seseorang dengan kunci publik. Kerahasiaan dan integritas email diperoleh dengan mengikuti enkripsi kunci publik-kunci pribadi. Dengan sertifikat digital yang diverifikasi oleh pihak ketiga tepercaya, nonrepudiation dari pengirim diperoleh.

Info Asset Security & Control

Soal A5-249 berkaitan dengan implementasi sistem untuk pertukaran email yang aman dengan pelanggan. Pilihan terbaik untuk memastikan kerahasiaan, integritas, dan nonrepudiation adalah opsi D, "Digital certificates" (Sertifikat digital). Sertifikat digital mengandung kunci publik dan informasi identifikasi tentang pemilik kunci publik tersebut. Kunci pribadi yang terkait disimpan secara aman oleh pemilik. Dengan menggunakan sertifikat digital yang diverifikasi oleh pihak otoritas yang terpercaya, kerahasiaan dan integritas email dapat dicapai melalui enkripsi dengan kunci publik-pribadi. Nonrepudiation diperoleh karena penggunaan tanda tangan digital, di mana hanya pemilik kunci pribadi yang dapat menghasilkan tanda tangan yang sesuai dengan sertifikat digital mereka. Ini sesuai dengan sub bab "Info Asset Security & Control" yang membahas enkripsi dan penggunaan kunci publik-privat.

250. Seorang auditor IS yang meninjau kontrol otentikasi dari sebuah organisasi seharusnya PALING khawatir jika:

A. akun pengguna tidak dikunci setelah lima kali upaya gagal.

B. kata sandi dapat digunakan kembali oleh karyawan dalam jangka waktu tertentu.

C. administrator sistem menggunakan kredensial login yang sama.

D. kedaluwarsa kata sandi tidak diotomatisasi.

Pembahasan:

A. Jika akun pengguna tidak dikunci setelah beberapa kali upaya gagal, serangan brute force dapat digunakan untuk mendapatkan akses ke sistem. Meskipun ini adalah risiko, pengguna biasa hanya memiliki akses sistem dibandingkan dengan seorang administrator.

B. Penggunaan kembali kata sandi adalah risiko. Namun, penggunaan kredensial login yang sama oleh administrator adalah risiko yang lebih parah.

C. Penggunaan kredensial login yang sama membuat akuntabilitas menjadi tidak mungkin. Ini terutama risiko dengan akun yang memiliki hak istimewa.

D. Jika kedaluwarsa kata sandi tidak diotomatisasi, kemungkinan besar karyawan tidak akan mengubah kata sandi mereka secara teratur. Namun, ini tidak separah kata sandi yang dibagikan, dan penggunaan kredensial login yang sama oleh administrator adalah risiko yang lebih parah.

Control type

Soal ini membahas tentang kontrol akses pengguna, khususnya risiko penggunaan kredensial login bersama oleh administrator sistem. Ini termasuk kontrol organisasi.