e) Auditing Audit terhadap suatu layanan atau data berarti menyelenggarakan proses pertanggung jawaban untuk setiap aksi yang terjadi pada sistem yang telah terotentikasi. Audit dapat mengawasi suatu sistem yang terotentikasi ketika segala proses berjalan normal maupun tidak ditinjau berdasarkan otorisasi yang telah diberikan kepada subyek yang telah ataupun tidak terotentikasi. Audit disebut juga proses merekam suatu objek atau subyek dengan tujuan menjaga kinerja sistem dan mekanisme keamanan. Audit dijalankan dengan membuat suatu sistem perekam kejadian dalam suatu catatan yang disebut dengan log. Audit juga dapat mengetahui terjadinya kerusakan sistem, misalnya kesaslahan program, rusaknya drive, atau terjadinya penyusupan, kegagalan sistem, perusakan terhadap suatu layakan, aksi yang tidak diijinkan atau yang bersifat asing semuanya disimpan dalam log.

f) Accountability Akuntabilitas adalah proses mengaitkan seorng pengguna dengan layanan keamanan dan implementasi dari mekanisme keamanan terhadap aktivitas yang terjadi pada suatu sistem. Seorang pengguna yang mengakses suatu sistem harus dapat diperhitungkan dan dipertanguungjawabakan. Suatu kebijakan keamanan dalam sistem dapat diterapakan dengan baik apabila akuntabilitas sistem dapat dijaga.

Akuntabilitas memberi kita sarana untuk melacak aktivitas di lingkungan kita kembali ke sumber mereka Selain itu, ini memberi kita sejumlah kemampuan, Bila diimplementasikan dengan benar, yang bisa sangat berguna dalam melakukan bisnis sehari-hari keamanan dan teknologi informasi di organisasi kami. Di Khususnya, organisasi perlu menjaga akuntabilitas dengan hati-hati agar dapat pastikan bahwa mereka mematuhi undang-undang atau peraturan yang terkait dengannya jenis data yang mereka tangani, atau industri tempat mereka beroperasi. Untuk memastikan bahwa kita memiliki akuntabilitas, kita memerlukan alat lain untuk masuktempat dan bekerja dengan baik. Akuntabilitas tergantung pada identifikasi, otentikasi,dan kontrol akses yang hadir sehingga kita bisa mengetahui siapa yang diberikantransaksi dikaitkan dengan, dan izin apa yang digunakan untuk mengizinkannya untuk melaksanakannya Dengan pemantauan dan penebangan yang tepat, kita sering bisa melakukannya dengan tepat ini dan tentukan, dalam waktu sangat singkat, rincian situasi yang dimaksud. Sangat mudah untuk melihat akuntabilitas dan alat audit yang terkait itu umumnya melekat padanya dan menganggapnya buruk karena mereka mirip dengan Big Brother yang melihat dari balik bahu kita. Dalam beberapa pengertian, ini Benar, dan pemantauan orang, tempat, dan hal-hal yang berlebihan dapat mengindikasikan lingkungan yang tidak sehat Kita juga bisa melangkah terlalu jauh ke arah lain. Jika kita melakukannya tidak memiliki kontrol yang memadai untuk mencegah atau mencegah hal-hal yang akan rusak aturan dan penyalahgunaan sumber daya yang mereka akses, kita bisa berakhir dengan buruk tempat juga Jika kita mempertimbangkan contoh skandal Enron pada tahun 2001, kita bisa melihat sebuah kasus dimana, karena kurangnya akuntabilitas kepada pemegang saham, dewan direksi, auditor, dan pemerintah A.S., Enron dapat menipu investornya dari miliaran dolar Inilah salah satu peristiwa yang mendorong pemberlakuan dari SOX, diarahkan secara khusus untuk menghentikan praktik semacam itu. Dalam beberapa kasus, seperti Ini, akuntabilitas sama dengan batas transparansi tertentu. Dalam beberapa situasi, Kegiatan kita harus transparan kepada pihak-pihak tertentu, seperti pemegang saham, untuk meminta pertanggungjawaban atas tindakan kami. Transparansi seperti itu didikte oleh hukum di perusahaan yang diperdagangkan. Kita mungkin juga melihat kasus di mana pertanggungjawaban diminta oleh agen luar, namun dorongan untuk mematuhi persyaratan ini harus berasal dalam organisasi kita. Kita bisa melihat contoh ini dalam persyaratan untuk memberi tahu mereka yang memiliki informasi pribadi atau keuangan yang terpapar dengan cara yang tidak sah dalam pelanggaran keamanan. Pelanggaran seperti itu tampaknya terjadi dengan keteraturan yang mengganggu, dan pada umumnya kita dapat menemukan contoh saat ini satu melalui pencarian singkat media berita. Saat sebuah perusahaan mengalami sebuah pelanggaran di Amerika Serikat, akan sering diwajibkan, oleh undang-undang, untuk memberi tahu mereka yang informasinya telah terpapar. Dalam banyak kasus, bagaimanapun, pelanggarannya adalah Tidak diketahui dari luar perusahaan oleh lebih dari sedikit orang, sampai mereka sebenarnya diumumkan kepada mereka yang terlibat langsung. Kita pasti bisa melihatnya di mana organisasi semacam itu mungkin tergoda, dalam kasus seperti itu, untuk tidak mengatakan apapuntentang kejadian tersebut Meskipun pelanggaran tersebut mungkin tidak segera terlihat oleh orang-orang di luar organisasi, atau pernah terlihat, dalam hal ini, kita masih bertanggung jawab untuk patuh dengan hukum yang mengatur pelanggaran di lokasi kami dan dengan undang-undang apa pun mengatur penanganan data dimana kita menjalankan bisnis. Dalam kasus ini dimana kita tidak melakukan diri kita dengan benar seperti berhubungan dengan hukum-hukum ini, kita mungkin begitu mampu melanjutkan bisnis seperti biasa untuk jangka waktu tertentu, tapi akhirnya kita akan ditemukan dan dampaknya pada pribadi, bisnis, dan hokum indra akan jauh lebih besar karena tidak menangani situasi dengan baik posisi pertama.

Manfaat Keamanan Akuntabilitas

Menerapkan akuntabilitas sering membawa serta sejumlah fitur bermanfaat dari perspektif keamanan. Saat kami menerapkan pemantauan dan pembalakan sistem dan jaringan kita, kita bisa menggunakan informasi ini untuk mempertahankan yang lebih tinggi postur keamanan daripada kita bisa sebaliknya. Secara khusus, alat itu memungkinkan pertanggungjawaban kita juga memungkinkan nonrepudiation, menghalangi yang akan melakukannya menyalahgunakan sumber daya kami, membantu kami dalam mendeteksi dan mencegah gangguan, dan membantu kami dalam menyiapkan materi untuk proses hukum.

Nonrepudiasi

Nonrepudiasi mengacu pada situasi di mana ada bukti yang cukup untuk mencegah seseorang dari berhasil menyangkal bahwa ia telah dibuat sebuah pernyataan, atau mengambil tindakan. Dalam pengaturan keamanan informasi, ini bisa jadidicapai dengan berbagai cara. Kita mungkin bisa menghasilkan bukti dari aktivitas langsung dari sistem atau log jaringan, atau mengembalikan bukti tersebut melalui penggunaan pemeriksaan forensik digital terhadap sistem atau perangkat yang terlibat. Kita mungkin juga bisa membangun nonrepudiation melalui penggunaan enkripsi teknologi, lebih khusus lagi melalui penggunaan fungsi hash yang bisa digunakan untuk menandatangani komunikasi atau file secara digital. Kita akan membahas metode seperti itu pada panjang yang jauh lebih besar di Bab 5 saat kita membahas enkripsi. Sebuah Contohnya mungkin sistem yang secara digital menandai setiap e-mail yang dikirim darinya, sehingga tidak ada kemungkinan penyangkalan yang mungkin terjadi terkait dengan pengiriman pesan yang dimaksud

Pencegahan

Akuntabilitas juga bisa menjadi penghalang besar terhadap perilaku tidak baik di Indonesia lingkungan kita Jika yang kita monitor sadar akan fakta ini, dan memang sudah begitu dikomunikasikan kepada mereka bahwa akan ada hukuman karena bertindak melawan peraturan, Orang-orang ini mungkin berpikir dua kali sebelum menyimpang dari luar garis. Misalnya, jika, sebagai bagian dari kegiatan pemantauan kami, kami melacak lencana Waktu akses untuk saat karyawan kami masuk dan keluar dari fasilitas kami, kami bisa Memvalidasi aktivitas ini melawan waktu yang mereka berikan pada kartu waktu mereka untuk setiap minggu, untuk mencegah karyawan kami memalsukan waktunya kartu dan menipu perusahaan untuk membayar tambahan dan tidak patut. Sementara ini sepertinya bisa mengalahkan Big Brother untuk beberapa orang (seperti, mungkin, seharusnya), semacam itu Metode yang sering digunakan di daerah dengan jumlah karyawan yang bekerja cukup tinggi shift, seperti yang dijalankan technical support help desks.

Intrusion Detection and Prevention

Salah satu motivasi di balik pembalakan dan pemantauan di lingkungan kita adalah untuk mendeteksi dan mencegah intrusi baik dalam arti logis maupun fisik. Jika kita menerapkan peringatan berdasarkan aktivitas yang tidak biasa di lingkungan kita dan memeriksa Informasi yang kami logikan secara reguler, kami berdiri jauh lebih baik kesempatan untuk mendeteksi serangan yang sedang berlangsung dan mencegahnya kita bisa melihat prekursor. Terutama di alam logis dimana serangan bisa terjadi dalam pecahan a Kedua, kita juga bijak menerapkan alat otomatis untuk melakukan hal tersebut tugas. Kita bisa membagi sistem seperti itu menjadi dua kategori utama: deteksi intrusi sistem (IDSes) dan sistem pencegahan intrusi (IPSes). IDS melakukan secara ketat sebagai alat pemantau dan peringatan, hanya memberi tahu kami bahwa sebuah seranganatau aktivitas yang tidak diinginkan sedang berlangsung. IPS, sering bekerja dari informasi yang dikirim oleh IDS, sebenarnya bisa mengambil tindakan berdasarkan apa yang terjadi di lingkungan Hidup. Sebagai tanggapan atas serangan melalui jaringan, sebuah IPS mungkin menolak lalu lintas dari sumber serangan. Kita akan membahas IDSes dan IPSes lebih besar panjang di Bab 7, 8, dan 10.

Tidak diperkenankannya Rekaman

Saat kami ingin mengenalkan catatan di lingkungan hukum, seringkali lebih mudah lakukan dan mintalah mereka diterima saat diproduksi dari yang diatur dan sistem pelacakan yang konsisten Misalnya, jika kita berusaha mengirimkan forensik digital bukti bahwa kami telah mengumpulkan untuk digunakan dalam kasus pengadilan, bukti kemungkinan besar akan terjadi tidak dapat diterima di pengadilan kecuali kita dapat memberikan yang solid dan terdokumentasi rantai hak asuh untuk bukti tersebut. Kita harus bisa menunjukkan di mana buktinya Setiap saat, bagaimana tepatnya hal itu berpindah dari satu orang ke orang lain, caranya itu dilindungi saat disimpan, dan sebagainya. Metode akuntabilitas kami untuk pengumpulan bukti, jika benar diikuti, akan Mudah-mudahan mari kita lihat rantai peristirahatan yang tak terputus ini. Jika kita tidak bisa mendemonstrasikannya Ini, bukti kita kemungkinan hanya akan dianggap sebagai desas-desus, paling banter melemahkan kasus kami, dan mungkin menempatkan kami di sisi yang kalah di pengadilan.

Bagaimana Kami Mencapai Akuntabilitas

Seperti yang telah kita diskusikan, kita dapat mencoba untuk memastikan akuntabilitas dengan meletakkannya peraturan dan memastikan bahwa mereka sedang diikuti. Sementara itu semua baik dan baik untuk memberi seseorang peraturan dan memintanya untuk mengikutinya, kita akan sering melakukannya perlu mengambil langkah lebih lanjut untuk memastikan bahwa ini benar-benar terjadi. Kita dapat lihat mekanisme seperti itu di dunia penegakan hukum. Geografisnya daerah di mana kita hidup telah meletakkan undang-undang tertentu untuk rakyatnya mengikuti. Seringkali, kita bisa menemukan hukum yang mengatur pencurian, membahayakan orang lain, operasi yang aman kendaraan, dan masih banyak lagi. Kami kemudian memiliki polisi yang memastikan kepatuhan terhadap undang-undang ini, baik secara reaktif maupun proaktif. Dalam dunia informasi Keamanan, kita sering menggunakan alat teknologi untuk melakukan tugas serupa.

Auditing

Salah satu cara utama kita dapat memastikan akuntabilitas melalui teknis Artinya adalah dengan memastikan bahwa kita memiliki catatan akurat tentang siapa yang melakukan apa dan kapan mereka melakukannya. Di hampir lingkungan manapun, dari tingkat teknologi terendah Yang tertinggi, akuntabilitas sebagian besar dilakukan melalui penggunaan audit dari beberapa variasi. Kamus Hukum Merriam-Webster mendefinisikan sebuah audit sebagai "a pemeriksaan metodis dan review "[2]. Kami mengaudit salah satu dari beberapa alasan. Auditing memberi kami data yang bisa kita terapkan akuntabilitas. Jika kita tidak memiliki kemampuan untuk menilai Aktivitas kita selama periode waktu tertentu, kita tidak memiliki kemampuan untuk memfasilitasi akuntabilitas dalam skala besar. Terutama di organisasi yang lebih besar, kapasitas kita Mengaudit secara langsung setara dengan kemampuan kita untuk meminta pertanggungjawaban siapa pun. Kita juga bisa terikat oleh persyaratan kontrak atau peraturan yang memaksa kita harus melakukan audit atas dasar reoccurring. Dalam banyak kasus, semacam itu audit dilakukan oleh pihak ketiga yang tidak terkait dan independen yang disertifikasi dan diberi wewenang untuk melakukan tugas semacam itu. Contoh bagus dari audit semacam itu adalah keputusan Diamanatkan oleh SOX, yang ada untuk memastikan bahwa perusahaan jujur melaporkan hasil keuangan mereka.

Apa yang Kami Audit?

Saat kita melakukan audit ada beberapa item yang bisa kita periksa, utamanya berfokus pada kepatuhan terhadap hukum dan kebijakan yang relevan. Dalam informasi dunia keamanan, kita cenderung melihat akses ke atau dari sistem sebagai primer fokus, tapi sering memperpanjang ini ke bidang lain juga, seperti keamanan fisik. Sandi adalah item yang diaudit, karena kami harus menetapkan kebijakan mendikte bagaimana mereka dibangun dan digunakan Seperti yang telah kita bahas dalam "Authentication" bagian dalam Bab 2, jika kita tidak berhati-hati untuk membuat kata sandi dengan aman Dengan cara itu, mereka bisa dengan mudah di-crack oleh penyerang. Kita juga harus khawatir dengan frekuensi di mana password diubah. Jika kita memang terjadi Untuk memiliki password jatuh ke tangan seseorang yang seharusnya tidak memilikinya, kita ingin mengganti password pada interval yang relatif sering untuk memastikan bahwa orang ini tidak memiliki akses permanen. Dalam banyak kasus, memeriksa kata sandi kekuatan dan pengelolaan perubahan kata sandi dilakukan secara otomatis mode oleh fungsi dalam sistem operasi atau oleh utilitas yang dirancang untuk melakukannya, dan ini perlu diaudit juga untuk memastikan bahwa mereka berada di tempat dan dikonfigurasi dengan benar. Lisensi perangkat lunak adalah topik audit umum lainnya. Terutama pada system dimiliki oleh organisasi tempat kami bekerja, memastikan semua perangkat lunak kami yang dilisensikan dengan tepat merupakan tugas penting. Jika kita akan diaudit oleh agen luar-Business Software Alliance (BSA), misalnya-dan kami ditemukan menjalankan sejumlah besar perangkat lunak tanpa izin, keuangan Hukuman bisa sangat berat. Hal ini sering terbaik jika kita dapat menemukan dan benar Hal tersebut terjadi sebelum menerima pemberitahuan dari perusahaan eksternal seperti BSA. Penggunaan internet adalah barang yang sering diaudit dalam organisasi, seringkali sebagian besar fokus pada kegiatan kami di Web, meskipun mungkin termasuk pesan instan, e-mail, transfer file, atau transaksi lainnya. Dalam banyak kasus, organisasitelah mengkonfigurasi server proxy sehingga semua lalu lintas tersebut disalurkan melalui saja beberapa gateway untuk memungkinkan penebangan, pemindaian, dan penyaringan potensial lalu lintas seperti itu Alat semacam itu bisa memberi kita kemampuan untuk memeriksa bagaimana sebenarnya sumber daya sedang digunakan dan untuk mengambil tindakan jika disalahgunakan. Banyak organisasi, seperti yang telah kita sebutkan di sepanjang bab ini, menangani data yang sifatnya sensitif. Khususnya untuk data yang dibutuhkan oleh Hukum yang harus dilindungi, data medis menjadi contoh yang baik, kita harus mengambil langkah untuk memastikan bahwa kita mematuhi tindakan pengamanan yang harus dilakukan ada di tempat Secara khusus, kita sering terikat untuk memastikan akses ke hal tersebut data dilakukan dengan cara yang berwenang, bahwa setiap persyaratan untuk data retensi selama periode waktu terpenuhi, dan data tersebut dihancurkan dengan aman bila sudah tidak dibutuhkan lagi Data tersebut sering ditempatkan di beberapa database, sebagian besar memiliki fasilitas built-in untuk pengendalian dan pemantauan akses pada tingkat yang sangat rinci.

Pembalakan

Penebangan memberi kita sejarah aktivitas yang telah terjadi di lingkungan sedang login Kami biasanya menghasilkan log dengan mode otomatis sistem operasi, dan melacak aktivitas yang berlangsung pada kebanyakan komputasi, jaringan, dan peralatan telekomunikasi, dan juga kebanyakan peralatan lainnya perangkat yang dapat dianggap jarak jauh untuk digabungkan atau dihubungkan ke komputer. Logging adalah alat reaktif, karena memungkinkan kita untuk melihat catatan dari apa terjadi setelah itu terjadi. Agar segera bereaksi terhadap sesuatu Dengan demikian, kita perlu menggunakan alat lebih banyak lagi di sepanjang garis IDS / IPS. Mekanisme penebangan sering dikonfigurasi dan dapat diatur untuk mencatat apapun dari peristiwa kritis semata, yang khas, untuk setiap tindakan yang dilakukan oleh sistem atau perangkat lunak, yang biasanya hanya dilakukan untuk tujuan pemecahan masalah ketika kita melihat sebuah masalah Kita akan sering menemukan kejadian seperti kesalahan perangkat lunak, kegagalan perangkat keras, pengguna masuk atau keluar, akses sumber daya, dan tugas yang dibutuhkan meningkatkan hak istimewa di kebanyakan log, tergantung pada pengaturan logging dan sistem yang dimaksud Log umumnya hanya tersedia bagi administrator sistem untuk ditinjau dan biasanya tidak dapat dimodifikasi oleh pengguna sistem, mungkin dengan kecuali menulis kepada mereka. Sangat penting untuk dicatat bahwa mengumpulkan kayu bulat Tanpa mengulasnya adalah tugas yang cukup sia-sia. Jika kita tidak pernah meninjau isi dari Kayu gelondongan, mungkin kita juga belum mengumpulkannya. Itu penting bahwa kita menjadwalkan review rutin log kita untuk menangkap apapun tidak biasa isinya Kita mungkin juga diminta untuk menganalisis isi log dalam kaitannya dengan yang tertentu kejadian atau situasi Jenis aktivitas ini sering jatuh ke petugas keamanan dalam kasus investigasi, insiden, dan pemeriksaan kepatuhan. Dalam kasus-kasus ini, Ini bisa menjadi tugas yang sulit jika periode waktu yang dimaksud lebih besar dari sedikit hari. Bahkan mencari isi log yang relatif sederhana, seperti yang dihasilkan oleh server proxy Web, bisa berarti memilah-milah sejumlah besardata dari satu atau lebih server Dalam kasus seperti itu, custom scripts atau bahkan tool semacam itu sebagai grep bisa sangat berharga untuk menyelesaikan tugas tersebut dalam jumlah yang wajar dari waktu.

Pemantauan

Pemantauan adalah bagian dari audit dan cenderung berfokus pada pengamatan informasi tentang lingkungan yang dipantau untuk menemukan hal yang tidak diinginkan kondisi seperti kegagalan, kekurangan sumber daya, masalah keamanan, dan tren itu mungkin menandakan datangnya kondisi seperti itu. Pemantauan sebagian besar bersifat reaktif aktivitas, dengan tindakan yang diambil berdasarkan data yang dikumpulkan, biasanya dari log yang dihasilkan oleh berbagai perangkat. Meskipun kita mungkin mempertimbangkan bagian analisis tren penebangan menjadi aktivitas proaktif, kita masih bereaksi terhadap keadaan sekarang untuk mencegah kondisi buruk daripada yang kita lihat saat ini. Saat melakukan pemantauan, biasanya kami melihat item data tertentu kami telah mengumpulkan, seperti penggunaan sumber daya pada komputer, latensi jaringan, Jenis serangan tertentu berulang kali terjadi terhadap server dengan jaringan antarmuka yang terpapar internet, lalu lintas yang melewati fisik kita kontrol akses pada waktu yang tidak biasa, dan sebagainya. Sebagai reaksi terhadap hal tersebut Aktivitas terjadi pada tingkat di atas apa yang biasanya kita harapkan, disebut kliping Tingkat, sistem pemantauan kami mungkin dikonfigurasi untuk mengirim peringatan ke a administrator sistem atau petugas keamanan fisik, atau mungkin akan memicu lebih banyak lagi Tindakan langsung untuk mengurangi masalah seperti menjatuhkan lalu lintas dari yang tertentu Alamat IP, beralih ke sistem cadangan untuk server kritis, memanggil undang-undang aparat penegak hukum, atau tugas sejenis lainnya.

Penilaian

Dalam beberapa kasus, audit kami mungkin mengambil rute yang lebih aktif untuk menentukan apakah semuanya sesuai dan sesuai dengan hukum, peraturan, atau kebijakan. Dalam kasus seperti itu, mungkin kita merasa perlu untuk memeriksa dengan saksama lingkungan kita untuk kerentanan. Kita bisa mengambil dua pendekatan utama untuk itu kegiatan: penilaian kerentanan dan pengujian penetrasi. Sementara istilah ini sering digunakan secara bergantian, sebenarnya ada dua rangkaian kegiatan yang berbeda. Penilaian kerentanan umumnya melibatkan penggunaan alat pemindaian kerentanan, seperti Nessus, A seperti yang ditunjukkan pada Gambar 4.2, untuk menemukan kerentanan semacam itu. Alat seperti itu umumnya bekerja dengan memindai sistem target untuk menemukan port mana terbuka pada mereka, dan kemudian menginterogasi setiap port terbuka untuk mencari tahu dengan tepat Layanan mana yang sedang mendengarkan di pelabuhan yang dimaksud. Dengan informasi ini, alat penilaian kerentanan kemudian dapat berkonsultasi dengan database kerentanannya informasi untuk menentukan apakah ada kerentanan yang mungkin ada. Meskipun Database alat semacam itu cenderung agak menyeluruh, serangan baru atau lebih baru Mereka yang digunakan sangat hemat oleh penyerang akan sering lolos dari pemberitahuan mereka. Sebagai metode yang lebih aktif untuk menemukan celah keamanan, kami mungkin juga ingin melakukan pengujian penetrasi Uji penetrasi, meski bisa menggunakan kerentanan Penilaian sebagai tempat awal, mengambil beberapa langkah langkah lebih jauh. Ketika kita Melakukan tes penetrasi, kita meniru, sedekat mungkin, teknik an penyerang sebenarnya akan menggunakan Kami mungkin berusaha mengumpulkan informasi tambahan pada lingkungan target dari pengguna atau sistem lain di sekitarnya, eksploitasi kelemahan keamanan dalam aplikasi berbasis Web atau database yang terhubung dengan Web, lakukan serangan melalui kerentanan unpatched dalam aplikasi atau sistem operasi, atau metode serupa. Kita akan membahas pengujian penetrasi pada panjang yang lebih besar Bab 8, 9, dan 10. Tujuan utama dalam melakukan penilaian terhadap kedua jenis adalah untuk menemukan dan memperbaiki kerentanan sebelum penyerang lakukan. Jika kita bisa melakukannya dengan sukses dan pada a Secara reoccurring, kami akan meningkatkan postur keamanan dan stand kami kesempatan yang jauh lebih baik untuk melawan serangan. Seperti halnya tindakan pengaman apa pun kita dapat diterapkan, penilaian keamanan hanya merupakan komponen tunggal dalam keseluruhan kami strategi defensif