MODUL PERKULIAHAN

EDP Audit

KEAMANAN LOGIS

(Logical Security)

Abstract

Modul ini berisi tentang Identifikasi atas risiko signifikan yang dihadapi sistem terbaik dapat dicapaimelalui proses penilaian risiko formal. Karena banyak auditor internal dan eksternalmenyiapkan dokumen penilaian risiko sebagai bagian dari proses audit mereka, standarmereka dapat menjadi sumber yang baikbagi tim desain sistem untuk membantumelakukan penilaian risiko formal

Kompetensi

Mahasiswa mampu pememahami tentang logical security, jenis-jenis logical security dan contoh-contoh kasus yang ada.

Pengantar

Kunci awal untuk melindungi sistem informasi dari akses yang tidak sah terletak pada desain dan pemrograman kontrol keamanan logis kedalam sistem, apakah itu sistem operasi, system manajemen database (DBMS), atau program aplikasi. Sebelum kontrol keamanan logis dirancang, pertama tim proyek desain harus menyadari risiko signifikan yang mungkin ada pada sistem. Tingkat risiko akan berdampak pada jenis kontrol keamanan logis yang perlu dirancang dalam sistem serta jumlah kontrol dan kekuatan relatifnya. Sistem berisiko tinggi jelas menjamin waktu dan sumber daya untuk merancang sejumlah besar kontrol keamanan logis yang kuat dari pada sistem berisiko rendah.

Desain Keamanan Logis

Identifikasi atas risiko signifikan yang dihadapi sistem terbaik dapat dicapaimelalui proses penilaian risiko formal. Karena banyak auditor internal dan eksternalmenyiapkan dokumen penilaian risiko sebagai bagian dari proses audit mereka, standarmereka dapat menjadi sumber yang baikbagi tim desain sistem untuk membantumelakukan penilaian risiko formal. Karena anggota tim desain biasanyaterdiri dari wakil-wakil dari semua daerah yang terkena dampak signifikan dalam organisasiyang ahli di bidangnya, tim kemungkinan akan mampu mengidentifikasisebagian besar risiko usaha yang signifikan. Namun, auditor sering menyadari risikobahwa sebuah tim desain mungkin tidak harus dipertimbangkan.

Sebagai contoh, salah satu risiko yang paling sulit dikontrol adalah kinerjaaktivitas yang tidak sah oleh administrator keamanan sistem. Menurut definisi, administrator keamanan sistemperlu menambah, menghapus, dan mengubah pengguna dankemampuan akses, memonitor dan mengatur aktivitas sistem, mengontrol parameter keamanan sistem, meninjau keamanan sistem dan catatan operasional, dan melakukanberbagai tugas lain yang tidak dilarang. (Catatan: dalam organisasi besar, beberapa di antara tugas tersebutmungkin dipisahkan.) Untuk menyelesaikan tugas-tugas ini, administrator keamanansistem membutuhkan akses yang hampir tidak terbatas dalam sistem. Sebagian besar anggota tim desaintidak berpikir dua kali mengenai fakta bahwa administrator keamanan sistem pada dasarnyaakan memiliki kebebasan atas sistem. Dalam kasus ini, merupakan tanggung jawab auditor untuk membuat sebagian dari tim desain sadar akan risiko yang ditimbulkan olehadministrator keamanan sistem. Tantangan yang dihadapi tim desain adalah apakahrisiko dari administrator keamanan sistem melakukan aktivitas tak terbatasmelampaui biaya perancangan kontrol untuk membatasi fungsi yangadministrator keamanan sistemdapat lakukan.[1]Dua teknik dirancang ke dalam sistem untuk kontrolaktivitas administrator keamanan sistem:

1. Memprogram sistem membutuhkan administrator keamanan sistem keduauntuk mengkonfirmasikan penambahan, perubahan, dan penghapusan ID pengguna dankemampuan aksesnya serta membuat perubahan sistem operasi dan parameter keamanan.Kontrol ini akan secara efektif mencegah satu administratorkeamanan sistem dari melakukan aktivitas yang tidak sah. Namun, kelemahankontrol ini adalah membutuhkan dua administrator keamanan sistem untukmengatasi setiap perubahan

yang berhubungan dengan keamanan pada sistem yang dapat menyebabkan penundaan operasional yang signifikanjika dua administrator keamanan sistem tidak adaketika muncul situasi yang memerlukan tindakan segera.

2. Memprogram sistem untuk mencatat semua potensi kejadian yang terkait keamanan sistem danmenerapkan prosedur dimana pencatatan ditinjau secara teratur atasaktivitas yang tidak biasaatau tidak sah, sebaiknya dilakukan oleh manajer administrator keamanan sistem. Kejadian pencatatan tersebut adalah penambahan, penghapusan, danperubahan ID pengguna dan kemampuan aksesnya (termasuk perubahansistem ID pengguna), inisialisasi ulang sistem, perubahan sistem operasi danparameter keamanan, upgrade perangkat lunak, kegagalan upaya masuk (*sign* on),mengeset ulang ID pengguna ketika pengguna lupa sandinya, dan kegiatan lainnyayang bisa mempengaruhi keamanan sistem. Pencatatan kejadian ini akan memberikanjejak audit aktivitasadministrator keamanan sistem, pengguna lainnya, dan hacker yang mencoba untuk menyusup sistem.

Sistem juga dapat diprogram sehingga administrator keamanan sistem tidak bias menghapus atau mengubah berkas catatan (yaitu, berkas catatan harus *read-only*),bahkan pada tingkat sistem operasi. Dengan cara ini, administrator keamanan sistem tidak dapat menghapus bukti jejak audit atas aktivitas yang tidak sah dari pencatatan. Sistem harus diprogram lebih lanjut untuk pengarsipan otomatis berkas catatan secara periodik (misalnya, bulanan) dan kemudian membersihkan berkas yang diarsipkan setelahwaktu yang cukup (misalnya, setiap tahun atau kurang sering, tergantung pada kekritisan informasi). Selain itu, berkas catatan dapat disimpan pada perangkat penyimpanan permanen seperti kompakdisk (CD) melalui drive WORM (menulis sekali dibaca banyak). Administrator keamanan sistem tidak harus memilki akses fisik ke CD di driveWORM.Jika administrator keamanan sistem tahu bahwa aktivitas mereka secara otomatis sedang direkam dan kemudian ditinjau oleh atasan mereka, kemungkinan jauh lebih kecil untuk mereka melakukan aktivitas yang tidaksah.

Meskipun pencatatan dapat menjadi penghalang untuk melakukan aktivitas yang tidak sah,hal ini bukan merupakan kontrol pencegahan. Sebaliknya, pencatatan adalah kontrol detektif yang akan mengidentifikasipelanggaran potensial setelah itu terjadi. Konsekuensi lain daripencatatanaktivitas terkait keamanan sistem adalah memerlukan jumlah tertentuatas kapasitas pengolahan sistem dan ruang penyimpanan disk. Jika volume aktivitas sangattinggi, "pengeluaran tambahan" dapat menurunkan kinerja sistem. Untuk

menghindari masalah ini,sistem dirancang dengan parameter yang membolehkanadministrator keamanan sistemuntuk mengurangi, tapi tidak menghilangkan, masa waktu berkas catatan yangdiarsipkan. Selain itu, sistem diprogram agarpencatatan hanya merekam jenis aktivitas yang paling berisiko terkait dengan keamanan sistem (misalnya, menambahkan pengguna dengankemampuan sistem administrasi, inisialisasi ulang sistem). Masalah ketigadari pencatatan ini adalah sulit untuk mencegah administrator keamanansistem dari kemampuan mengakses dan menghapus berkas catatan, atau berkas lainnya, pada tingkat sistem operasi. Hal itu mungkin untuk menyamarkan berkas catatan atau berkas lain sehingga sulit ditemukan, tapi administrator keamanan sistem yang berpengalaman mungkin masih dapat menemukannya. Lihat studi kasus 8.1 untuk kasus bagaimana berkas catatan membantu mengidentifikasitindakan penipuan oleh administrator keamanan sistem. Juga, lihat studi kasus15.3, yang menjelaskan beberapa kesulitan yang harus dihadapi dalam desain keamanan pada proyek sistem informasi yang kompleks.

STUDI KASUS 8.1

Identifikasi Tindakan Penipuan oleh Pencatatan

Selama audit aplikasiutama pinjamandan deposit di suatu lembagakeuangan, manajerpengolahan data (DP) diminta untuk mencetak daftar semua pengguna dan kemampuan aksesnya. Dari hasil cetakan, parapengguna yang memiliki kemampuan administrator keamanan sistem telah di identifikasi. Di cabang tertentu,staf operasi DP danmanajer DP melakukan tugas administrasi keamanan. Oleh karena itu, ketika hasil cetakan dari semua pengguna dan kemampuan akses diteliti, ditemukan bahwa staf DP operasi dan manajer DP tersebut mempunyai kemampuan administrator keamanan sistem, seperti yang diharapkan.

Dua analis sistem perangkat lunak dari departemen DP diharapkan ditemukan di cetakan. Analisis tidak memerlukan kemampuan sistem administrasi sebagai bagian dari tugas-tugasnya.Namun, melaluidiskusi informal dan hubungan sebelumnya dengan Departemen DP, ditemukan bahwa mereka secara rutin melakukan tugas tersebut untuk membantu daerah operasi DP dan memperlancar pekerjaan mereka baik database langsung maupun percobaan. Peninjauan cetakan menampilkan kemampuan akses dari 2 orang

analis tersebut mengungkapkan bahwa mereka tidak memiliki kemampuan administrasi sistem keamanan.

Panduan administrasi keamanan sistem kemudian disebutkan, dan dicatat bahwa aplikasi secara otomatis mencatat semua perubahan yang terkait dengan sistem keamanan, termasuk perubahan kemampuan akses pengguna.Hasil cetakan dari catatan tersebut selama sebulan diminta dari manajer DP yang tidak menaruh curiga.Catatan menunjukkan perubahan yang didaftarkan dalam permintaan kronologis.Untuk setiap perubahan, catatan menunjukkan tanggal, waktu, perubahan yang dibuat, dan ID pengguna dari orang yang membuat perubahan tersebut.Catatan diuji untuk tanggal dan waktu segera sebelum tanggal dan waktu berjalan atas daftar pengguna dan kemampuan akses yang diterima dari manajer DP.Dicatat bahwa manajer DP tersebut menghapus kemampuan administrator keamanan sistem dari dua analis sistem perangkat lunak segera sebelum mencetak daftar pengguna dan kemampuan akses.

Saya membahas masalah tersebut dengan manajer saya.Untuk tiga alasan, kami memutuskan tidak menentang manajer DP mengenai perubahan yang bersifat penipuan.

1. Dengan menghapus kemampuan akses administrasi keamanan sistem dari analis sistem perangkat lunak, manajer DP.
2. Manajer DP harus merubah kembali kemampuan akses dari analis sistem perangkat lunak ke kemampuan administrasi keamanan sistem kapanpun.
3. Yang paling penting, kami menginginkan hubungan yang paling dekat dekat departemen DP. Kami merasa bahwa menentang manajer mengenai perubahanakanmencegah daripada membantu upaya kami. Karena manajer menghargai baik karyawannya, masalah tersebut hanya didokumentasikan dalam kertas kerja audit tidak dalam laporan manajemen.

Tergantung pada potensi risiko dari suatu sistem, tim desain mungkin ingin memasukkan satu atau kedua teknik pengendalian tersebut, serta yang lain, dalam persyaratan desain akhir mereka. Setelah menyelesaikan analisis risiko, tim desain dapat fokus pada jenis kontrol keamanan logis apa yang harus dimasukkan ke dalam sistem yang mereka kembangkan. Untuk menggambarkan bentuk umum keamanan logis lainnya yang mungkin perlu dirancang ke dalam sistem, mari kita lihat bagaimana sebuah sistem baru dibawa ke kehidupan.

MEMBAWA SISTEM BARU KE DALAM KEHIDUPAN

Setelah pemrograman dan instalasi selesai, administrator sistem keamanan atau teknisi instalasi menginisialisasi program eksekusi untuk mengaktifkan sistem untuk pertama kalinya.Sistem tersebut harus diprogram untuk mengenali ID pengguna sistem dan kata sandi awal.ID pengguna sistem dan sandi awal harus ditentukan dalam dokumentasi sistem dalam hal sistem harus diinisialisasi ulang di kemudian hari.Sistem harus diprogram seperti itu, dengan memasukkan ID pengguna sistem dan sandi awal, administrator keamanan sistem meminta untuk memasukkan sandi baru yang terdiri dari delapan atau lebih huruf-angka, karakter khusus.Dengan membolehkan kombinasi dari angka dan huruf khusus digunakan dalam sandi, jumlah kemungkinan kombinasi karakter meningkat secara signifikan.Panjang persyaratan minimum sandi lebih panjang untuk ID sistem pengguna yang diprogram ke dalam sistem berisiko tinggi.

Karakter sandi tidak boleh terlihat pada layar terminal sebagaimana dimasukkan oleh administrator keamanan sistem. Control ini disebut penyamaran sandi. Penyamaran sandi membuatnya sulit untuk orang yang berjalan dan pemerhati untuk mencuri sandi pengguna lain dan melakukan aktivitas yang tidak sah.

Sistem harus diprogram agar sandi tidak dapat dilihat oleh sadministrator keamanan sistem dari dalam aplikasi, sistem manajemen database (jika ada), atau pada tingkat sistem operasi. Untuk mengatasi hal ini, berkas sandi harus dienkripsi, menggunakan algoritma enkripsi yang relatif aman.Berkas enkripsi yang memadai jauh lebih sulit untuk diuji dan diubah seperti membandingkannya dengan berkas yang tidak terenkripsi.ID pengguna dan sandi harus tetap dalam keadaan terenkripsi karena mereka ditransmisikan melalui jaringan telekomunikasi. (*Catatan :* Lihat pembahasan kriptografi pada Bab 11.)

ID pengguna sistem harus diprogram memiliki kemampuan administrasi keamanan sistem yang memungkinkan administrator keamanan sistem untuk memasuki operasi yang disesuaikan dan parameter keamanan dan untuk membuat ID pengguna bagi pengguna lain dalam sistem. Ketika penambahan ID pengguna dibuat, sistem harus memberinya kemampuan akses *read-only* sebagai standar, sebagai lawan pemberian kemampuan akses

universal.Kontrol desain memastikan bahwa upaya penambahan harus dilakukan sebelum ID pengguna baru dapat membahayakan.

Sistem harus diprogram untuk memungkinkan administrator keamanan sistem menetapkan sandi awal setidaknya delapan karakter bagi setiap ID pengguna baru.Ketika pengguna mengakses untuk pertama kalinya, sistem harus meminta pengguna untuk merubah sandinya. Dalam hal ini, administrator keamanan sistem dicegah dari mengetahui sandi pengguna lain (asumsikan bahwa berkas sandi telah terenkripsi secara memadai).

Jumlah dan jenis parameter operasi yang disesuaikan akan sangat bervariasi, tergantung pada jenis aplikasi dan persyaratan pengguna yang ditentukan selama tahap desain. Jumlah dan jenis parameter keamanan sistem yang disesuaikan akan juga bervariasi dengan aplikasi, tergantung pada risiko aplikasi dan sumber daya dan keuangan yang tersedia selama perancangan dan pengembangan sistem. Parameter keamanan sistem harus disesuaikan pada dasar seluruh-sistem dan pada dasar pengguna individu.Lima parameter keamanan sistem seluruh-sistem yang disesuaikan umumnya adalah sebagai berikut.

1. ***Panjang minimum sandi***. Sistem harus menolak apapun upaya pengguna untuk memasuki sandi dengan karakter yang lebih sedikit daripada pengaturan parameter. Untuk kebanyakan sistem bisnis komersial, minimum panjang sandi cukup delapan karakter. Namun, jika sistem tersebut dalam dukungan proses yang sangat berisiko, karakter lebih akan diperlukan, bahkan dalam kisaran 20 lebih. Dengan sandi yang panjang, frase kata biasanya dibutuhkan. Sebuah frase kata adalah pernyataan sederhana yang hanya diketik dengan kata tunggal. Frase kata dapat sangat efektif karena mereka meminta pengguna yang tidak sah untuk menebak pernyataan konsep yang hanya dengan kata tunggal. Mereka juga efektif melawan perangkat lunak "peretakan" kamus. Beberapa sistem memiliki parameter yang memungkinkan administrator keamanan sistem mengharuskan pengguna memasukkan satu atau lebih angka atau karakter khusus dalam sandi mereka.
2. ***Masa kadaluarsa sandi***. Ketika masa kadaluarsa sandi telah berlalu, sistem harus mengupayakan setiap pengguna untuk memasukkan sandi lama serta sandi baru dua kali berturut-turut. Bagi kebanyakan aplikasi komersial, masa kadaluarsa sandi cukup 60 hari. Lagi, dalam kasus sistem berisiko tinggi, perubahan sandi terlalu sering akan dibutuhkan. Perlu diingat bahwa jika sistem membolehkan pengguna memasukkan

sandi baru, kemudian merubahnya kembali ke sandi lama, efektivitas seringnya perubahan sandi dihilangkan.

3. ***Sejumlah upaya akses yang gagal berturut-turut dibolehkan sebelum menangguhkan ID pengguna***. Jika sejumlah upaya akses yang gagal berturut-turut telah tercapai, sistem harus menangguhkan ID pengguna. Penangguhan berarti ID pengguna tidak dapat digunakan selama administrator keamanan sistem menyetel ulang kembali ID pengguna ke status aktif. Ini merupakan kontrol yang sangat baik untuk mencegah *hacker* atau menerjang sistem dari percobaan mengakses pada jumlah waktu yang tak terbatas. Dalam kebanyakan kasus, menangguhkan ID pengguna cukup setelah tiga kali upaya akses yang gagal berturut-turut untuk tujuan poerasional dan keamanan.
4. ***Sepanjang hari dan hari dalam seminggu pengguna dapat mengakses***. Sistem harus menolak apapun upaya pengguna untuk mengakses sistem selama sepanjang hari atau hari dalam seminggu yang berada di luar pengaturan parameter. Kontrol ini membantu mencegah upaya akses yang tidak sah selama di luar jam kerja oleh orang yang memilik akses fisik ke fasilitas (misalnya custodian atau pengawas keamanan).
5. ***Masa tidak aktif diperbolehkan selama pengguna secara otomatis keluar akses***. Ketika ID pengguna tidak aktif untuk masa tertentu dalam parameter, sistem harus secara otomatis menyimpan dan menutup berkas apapun yang masih aktif, mengakhiri aplikasi, dan keluar akses pengguna. Kontrol ini mengurangi risiko akses tidak sah ketika pengguna meninggalkan tempat kerjanya dan lupa atau memilih untuk tidak mengeluarkan aksesnya. Yang paling tepat sesi batas waktu harus ditentukan berdasarkan keseimbangan antara kebutuhan operasional dan keamanan. Biasanya, masa sesi batas waktu 10 menit atau kurang harus disarankan.

Sistem harus diprogram untuk memungkinkan parameter keamanan sistem yang sama secara terpisah ditentukan pada dasar ID pengguna individu oleh administrator keamanan sistem. Jika parameter keamanan sistem yang tidak terpisah ditetapkan untuk ID pengguna tertentu, standar parameter keamanan sistem harus berlaku.Sistem harus menerapkan apapun parameter ID pengguna individu dalam preferensi atas parameter sistem standar.Logika ini memungkinkan administrator keamanan sistem untuk mengakomodasi pengguna yang memiliki kebutuhan akses yang unik tanpa mengubah pembatasan akses dari semua pengguna.Sebagai contoh, dalam kasus pengguna yang mengharapkan bekerja sepanjang akhir pekan untuk proyek khusus, administrator keamanan sistem menetapkan parameter akses ID pengguna individu untuk orang ini.

Contoh lain terjadi bila ID pengguna administrator keamanan sistem cadangan dibuat. Administrator keamanan sistem utama mungkin menginginkan pengaturan panjang minimum sandi untuk ID pengguna ini lebih tinggi jumlah minimum karakternya daripada standar untuk ID pengguna administrator keamanan non sistem.Kelima parameter keamanan sistem harus diterapkan ke semua ID pengguna administrator keamanan non sistem.Namun, parameter 1, 3, dan 4, tidak harus diterapkan pada ID pengguna sistem.

Sistem harus diprogram sehingga parameter seluruh-sistem dan minimalpanjang sandi individu tidak diterapkan untuk ID pengguna sistem. Alasannya adalah bahwa administrator keamanan sistem yang baru belum terbiasa dengan kebutuhan akan kontrol minimalpanjang sandiyang secara sengaja atau tidak sengaja menetapkan parameter ke minimal rendah yang tidak diinginkan, seperti tiga karakter. Kata sandi ID pengguna sistem kemudian dapat diubah menjadi hanya tiga karakter, sehingga mengekspos sistem dengan risiko yang lebih tinggi secara signifikan atas akses yang tidak sah.Hal ini juga bisa terjadi dalam kasus administrator keamanan sistem malas.Memiliki tersendiri, persyaratan pemrograman yang tidak bisa berubah bahwa sandi untuk ID pengguna sistem minimal delapan karakter gabungan huruf angka menghilangkan kemungkinan sandi yang terlalu pendek atau sederhana yang diberikan kepada ID pengguna sistem dan dengan demikian sangat mengurangi risiko akses yang tidak sah.

Parameter mengenai jumlah upaya akses yang gagal berturut-turut diperbolehkan sebelum menangguhkan ID pengguna yang juga tidak berlaku untuk ID pengguna sistem.Jika dilakukan, maka seseorang yang berusaha *hack*sandi untuk ID pengguna sistem dapat menyebabkannya ditangguhkan setelah hanya beberapa percobaan. Ini akan menjadi situasi yang sangat tidak diinginkan dalam hal administrator keamanan sistem tidak membuat cadangan ID pengguna sistem dan perlu melakukan fungsi yang bukan ID pengguna lain lakukan. Jika sistem ini diprogram sehingga ID pengguna sistem tidak dilindungi oleh kontrol penangguhan otomatis, kebutuhan untuk memprogram sistem dengan minimal perubahan panjang sandibagi ID pengguna sistem dari delapan atau lebih karakter gabungan huruf angka menjadi lebih kritis.

Parameter sepanjang hari dan hari dalam seminggu tidak harus diterapkan ke dalam ID pengguna sistem karena administrator keamanan sistem memerlukan akses kapan pun baik harian atau mingguan.Jika masalah kritis muncul selama waktu ketika ID pengguna sistem dibatasi, organisasi menderita kerusakan yang signifikan pada program sistem dan

data. Ini serupa dengan memiliki kunci waktu pada lemari besi bank dan kemudian ada api keluar dari dalam lemari besi tersebut. Seseorang tidak bisa membuka kunci waktu dan harus berharap agar oksigen habis sebelum uang tersebut terbakar.

Parameter 1, 3, dan 4 tetap harus diterapkan pada ID pengguna administrator keamanan sistem cadangan yang dibuat menggunakan ID pengguna sistem. Meskipun ID pengguna administrator keamanan sistem cadangan biasanya diberikan akses setara pada ID pengguna sistem, mereka tetap saja dibuatkan ID pengguna, yang bisa dihapus oleh ID pengguna sistem atau ID pengguna administrator keamanan sistem yang berbeda, dan yang dapat dihapus saat sistem diinisialisasi ulang. Ini menimbulkan masalah lain desain utama.

Sistem harus diprogram agar ID pengguna sistem tidak bisa dihapus.Sebagai contoh, salah satu administrator keamanan sistem cadangan secara sengaja atau tidak berusaha untuk menghapus ID pengguna sistem. Jika permintaan tersebut diizinkan, operasi penting dari sistem akan tergantung pada parameter akses sistem yang berlaku untuk ID pengguna administrator keamanan sistem cadangan. Jika parameter tidak dipahami dengan benar, seperti dalam kasus parameter sepanjang hari dan hari dalam seminggu, sistem mungkin tidak dapat diakses dalam hal masalah selama di luar jam.

Rincian dari kontrol akses sistem mengacu pada tingkat kekhususan dengan parameter dimana akses sistem dapat dikontrol. Pada tahap desain pada sistem, rincian harus ditentukan dengan jelas.Perlu diingat bahwa ada pertukaran antara rincian dan biaya, dalam hal peningkatan dolar dan waktu pemrograman dan biaya tambahan sistem setelah sistem diterapkan.Selain jenis khas di atas kontrol keamanan logis, lainnya, kontrol yang lebih rinci dapat dirancang ke dalam sistem. Keempat kontrol keamanan logis akan menambah rincian kontrol yang diberikan kepada administrator keamanan sistem:

1. Sandi harus dilindungi untuk mencegah pengguna dari memasukkan sandi yang ditebak dengan mudah. Contohnya, sistem diprogram dengan parameter perubahan untuk jumlah maksimum karakter berturut-turut yang dibolehkan. Dengan demikian, sandi seperti “aaaaaa” atau “111111” dapat dicegah.
2. Sistem harus diprogram untuk mensyaratkan minimal dua angka dan dua karakter non alphabet dalam sandi, sehingga membuat sandi lebih sulit ditebak.
3. Sistem harus diprogram untuk mencegah pengguna dari memasukkan sandi yang baru saja digunakan. Untuk mengatasi kontrol ini, sistem harus dicatat dalam format terenkripsi, jumlah yang ditetapkan pada sandi sebelumnya atas semua ID pengguna

(misalnya 10). Parameter kemudian dibuat yang membolehkan administrator keamanan sistem secara fleksibel mengatur angka sebelum "generasi" sandi sistem tidak akan membolehkan pengguna untuk menggunakannya kembali.

4. Sistem harus diprogram untuk membolehkan ID pengguna tertentu saja yang mengakses dari tempat kerja tertentu. Sebagai contoh, ID pengguna yang ditetapkan untuk personil operasi komputer tidak dapat diakses dari tempat kerja di departemen pemrograman, dan sebaliknya. Setiap perangkat (workstation, terminal, printer, gateway, dll) pada sistem diberikan sebuah nomor "simpul" unik dimana sistem dapat mengidentifikasinya. Untuk menerapkan pembatasan tempat kerja, administrator keamanan sistem akanmenetapkan tanda tertentu pada simpul atau rentang simpul untuk setiap ID pengguna. Sebuah usaha oleh pengguna untuk akses ke sejumlah simpul yang berbeda dari nomor simpul resminya atau di luar jangkauan yangsahakan ditolak.

Sistem harus diprogram untuk menerapkan kontrol rincian 1, 2, dan 3 pada semua ID pengguna, termasuk ID pengguna sistem. Namun, kontrol rincian 4 harus diterapkan pada semua ID pengguna kecuali ID pengguna sistem, dimana membolehkan untuk mengakses dari tempat kerja manapun agar dapat memecahkan masalah dan menjaga keamanan sistem dalam cara efektif dan efisien.

Penambahan kontrol rincian yang deprogram dalam beberapa sistem merupakan parameter akses sistem yang dapat diatur untuk membolehkan sesi akses yang bersamaan oleh pengguna. Sesi akses bersamaan adalah ketika ID pengguna yang sama diizinkan mengakses dari dua atau lebih tempat kerja secara serentak. Dari susut pandang operasional, fitur ini akan sangat bermanfaat. Sebagai contoh, administrator keamanan sistem mungkin mengakses pada tempat kerja normal mereka dan mungkin di tengah-tengah melakukan interaktif panjang permintaan database.Masalah keadaan darurat mungkin muncul, sehingga membutuhkan administrator keamanan sistem untuk melakukan beberapa macam tindakan segera (misalnya presiden perusahaan lupa sandinya dan perlu mengeset ulang segera). Daripada mengakhiri pekerjaan interaktif panjang dan kemudian harus memulainya kembali dari awal, jelas lebih efisien bagi administrator keamanan sistem pergi ke komputer lainuntuk melakukan operasi ulang. Namun, jenis kegiatan ini dapat memberikan kelemahan pengendalian yang signifikan. Dalam contoh ini, administrator keamanan sistem mungkin perlu menggunakan komputer di ruangan atau lokasi lain di dalam fasilitas. Sementara administrator keamanan sistem pergi, pekerjaan

interaktif bisa terselesaikan, sehingga membebaskan sesi akses administrator keamanan sistem di komputer aslinya.Pengguna yang tidak sah kemudian bisa melanjutkan untuk mengakses sistem dan melakukan fungsi administrasi keamanan sistem yang tidak sah (misalnya, membuat ID pengguna yang tidak sah dengan kemampuan administrator keamanan sistem untuk digunakan di lain waktu). Jika tiga atau lebih sesi bersamaan diperbolehkan, potensi untuk jenis akses yang tidak sah akanmeningkat secara drastis.

Oleh karena itu, pengguna akhir tidak harus diberikan kemampuan akses bersamaan karena sejumlah kelemahan keamanan potensial yang dapat timbul dalam lingkungan pengguna akhir. Jika diperlukan oleh kebutuhan operasional, hanya administrator keamanan sistem dan sangat mungkin memilih beberapa pengguna lain yang mungkin membutuhkankemampuan akses bersamaan. Jika demikian, tidak lebih dari dua sesi bersamaan harus diizinkan, dan kegiatan mereka harus dicatat dan ditinjau. Situasi yang paling aman akan mendesain dan memprogram sistem sehingga sesi akses bersamaan tidak diperbolehkan dan bahkan bukan parameter sistem keamanan opsional. Untuk mengatasi masalah tersebut harus menghentikan program atau permintaan interaktif yang memakan waktu beberapa menit untuk menyelesaikannya, administrator keamanan sistem atau pengguna yang bersangkutan harus menyerahkan pekerjaannya untuk pengolahan "*batch*".Sebuah program *batch* adalah salah satu yang diajukan oleh pengguna dan dieksekusi oleh sistem ketika sumber daya pengolahan data tersedia.Mengirim pekerjaan dalam *batch* membebaskan ID pengguna untuk melakukan fungsi interaktif lainnya tanpa harus menunggu pekerjaan terselesaikan.

Bahkan jika sistem dirancang agar sesi akses bersamaan bukan pilihan, administrator keamanan sistem dapat menghindari kontrol desain hanya dengan membuat beberapa ID pengguna untuk pengguna yang sama. Risiko dari satu pengguna yang memiliki dua atau lebih ID pengguna yang sama untuk pengguna yang sama memiliki kemampuan akses bersamaan. Oleh karena itu, praktik ini harus dicegah.

Kontrol keamanan logis hanya menggambarkan mengenai situasi desain sistem yang optimal. Namun, dalam kehidupan nyata, beberapa kontrol tidak akan didesain ke dalam sistem. Hal itu seperti sebagian kontrol telah ada, tetapi mempengaruhi ID pengguna sistem dengan cara yang dapat mengakibatkan peningkatan risiko akses yang tidak sah melalui ID pengguna sistem. Sebagai contoh, parameter minimal panjang sandi mungkin disetel untuk tingkat rendah dan mungkin diterapkan dalam ID pengguna sistem maupun semua

pengguna lainnya. Penambahan kontrol rincian yang mungkin atau tidak mungkin mempengaruhi ID pengguna sistem akan cenderung ditemui. Dalam setiap kasus, penilaian atas semua risiko dari proses dipengaruhi oleh sistem dan kemudian apakah kekurangan dari kontrol tertentu, atau cara dimana didesainnya, cukup signifikan untuk memerlukan saran memprogram ulang bagian yang ada dari sistem. Dalam beberapa kasus, kelemahan yang teridentifikasi dapat diatasi sebagian dan dengan benar oleh pengembang yang tepat dari keamanan sistem terkait kontrol.

ID DAN SANDI PENGGUNA

Seperti yang dapat kita lihat dari ilustrasi sebelumnya atas kontrol keamanan logis dalam sistem yang baru saja diinstal, ID pengguna dalam hubungannya dengan sandi membentuk satu dari yang paling umum dan jenis khusus dari kontrol keamanan logis.Karenanya, ID dan sandi pengguna diberikan di hampir setiap sistem komputer yang membutuhkan setidaknya beberapa bentuk dari keamanan. Tanpanya, hampir tidak ada seorangpun dapat mengakses sistem informasi dan melakukan transaksi yang tidak sah, memperoleh akses yang tidak sah ke informasi, merusak data dan program, mengeluarkan virus, menambah, merubah, dan menghapus pengguna dan kemampuan akses pengguna, membuat perubahan yang tidak sah pada operasi sistem dan parameter keamanan, dan melakukan banyak sekali kegiatan yang tidak diinginkan. Sayangnya, kehadiran yang lebih pada ID dan sandi pengguna tidak memastikan bahwa sistem informasi aman secara memadai.Semua kontrol keamanan logis, termasuk semua ID dan sandi pengguna, harus didesain hati-hati dan dijalankan efektif dengan benar.

KONTROL AKSES JARAK JAUH

Pada hari-hari awal komputasi, administrator keamanan sistem secara khusus merupakan pengguna yang hanya membutuhkan kemampuan akses ke sistem dengan jarak jauh.Pengolahan komputer dipusatkan, dan pengguna secara khusus mengakses menggunakan terminal bodoh.Hari ini semakin banyak pengguna meminta kemampuaan akses jarak jauh menggunakan lapotop, asistan personal digital (PDA), dan beberapa macam telepon selular. Mereka secara khusus meminta akses ke jaringan organisasi dan dari sana, mengakses ke banyak aplikasi. Akses jarak jauh memfasilitasi berbagai efisiensi dan

memungkinkan komunikasi dan penyelesaian pekerjaanlebih tepatwaktu, tapi hal ini juga secara signifikan meningkatkan risiko dalam jaringan organisasi dari sistem komputasi akses yang tidak sah, virus, dan tantangan operasional lainnya.Untuk membantu mengurangi risiko ini, sejumlah teknologi kontrol akses jarak jauh telah dikembangkan.Kontrol akses jarak jauh yang paling umum yaitu sirkit sewa khusus, panggilan kembali otomatis, sesi lapisan soket aman (SSL), otentikasi multifactor, dan jaringan pribadi virtual (VPN).Dalam beberapa situasi, gabungan dari satu atau lebih kontrol ini dikembangkan.Setiap kontrol ini dibahas secara singkat disini.Sebagian besar pada beberapa jenis teknologi enkripsi.Lihat Bab 11 untuk pembahasan rinci atas enkripsi dan kriptografi.

Sirkit sewa khusus adalah koneksi telepon yang bersifat privadi dalam arti bahwa perusahaan telekomunikasi penyewaan tidak membolehkan pihak eksternal untuk mengaksesnya.Data dibawa antara komputer di sirkit sewa khusus yang tidak dienkripsi olehstandar karena ada sedikit risiko intersepsi.Tergantung pada sifat dari informasi yang dipertukarkan, kontrol enkripsi terpisah mungkin perlu diterapkan.Sirkit sewa khusus ini mahal tapi memberikan kinerja yang tinggi karena kurangnya lalu lintas eksternal dan pengurangan kebutuhan untuk mengenkripsi semua lalu lintas internal.Pengguna jarak jauh masih harus dimintai otentikasi ke jaringan minimal menggunakan ID pengguna dan sandi.

Panggilan kembali otomatis adalah kontrol dimana modem komputer pengguna jarak jauhmemanggil nomor telepon yang dikhususkan untuk akses jaringan jarak jauh. Komputer jarak jauhmemberikan informasi identifikasi yang cukup sehingga sistem otentikasi dapat mengakhiri panggilan asli dan memanggil nomor telepon resmi secara otomatis dalam database untuk komputer jarak jauh tersebut.Kontrol ini membantu mencegah pengguna yang tidak sah dari mencoba mengakses jaringan organisasi, bahkan jika mereka mengetahui akses nomor telepon jaringan jarak jauh. Komputer otentikasi hanya akan memanggil nomor telepon yang belum resmi dalam databasenya. Setelah berhasil memanggil kembali, pengguna jarak jauh masih harus dimintai otentikasi ke jaringan minimal menggunakan ID dan sandi pengguna.Tergantung pada sifat aksesnya, lalu lintas data mungkin atau tidak mungkin perlu dienkripsi.

Lapisan soket aman adalah protokol yang digunakan untuk memberikan sesi internet terenkripsi antara komputer jarak jauh dan server jaringan.Biasanya berjalan pada port 443 dari server jaringan dan menggunakan enkripsi kunci publik untuk membentuk koneksi

terpercaya.Setelah sambungan berhasil dibuat, semua data yang dipertukarkan antara komputer jarak jauh dan server jaringan dienkripsi secara simetris.Kekuatan enkripsi tergantung pada panjang kunci simetris (biasanya 128 bit) yang didukung oleh browser komputer jarak jauh dan server jaringan.Enkripsi data konstan menggunakan kapasitas pemrosesan unit pengolahan pusat (CPU) yang cukup untuk menurunkan kinerja dari komputer jarak jauh dan server jaringan.Sementara SSL mengenkripsi data antara komputer jarak jauh dan jaringan, tidak memberikan bukti bahwa pengguna jarak jauh resmi memulai sesi.Pengguna jarak jauh masih harus dimintai otentikasi ke jaringan minimal menggunakan ID dan sandi pengguna.

Otentikasi multifaktor adalah implementasi dari dua atau lebih kontrol sebelum memberikan akses ke pengguna.Otentikasi dua faktor biasanya diterapkan untuk pengguna jarak jauh.Hal ini mengharuskan pengguna pertama mengotentifikasi ke server tantangan-respon dan kemudian mengotentifikasi ke server jaringan dengan jaringan ID dan sandinya.Untuk otentikasi ke server tantangan-respon, pengguna harus memiliki perangkat bukti. Selama proses otentikasi, pengguna ditantang untuk memasukkan nomor secara acak sekali pakai. Angka tersebut diperoleh dari perangkat bukti yang disinkronkan dengan server tantangan-respon saat penerbitan.Untuk mengakses bukti tersebut, terlebih dahulu pengguna harusmemasukkan PIN. Tiga produk umum yang menyediakan jenis kontrol teknologi informasi internal yaitu SecurID® oleh RSA Security Corporation, Defender® oleh Symantec Corporation, dan CRYPTOCard® oleh CRYPTOCard Corporation. Contoh dari otentikasi tiga faktor meminta pengguna untuk memberikan kepemilikan biometrik (misalnya, jari, telapak tangan, retina, iris, suara, dll) sebagai tambahan proses otentikasi dua faktor. Jelas, perangkat keras dan perangkat lunak yang berlaku perlu diterapkan pada klien dan server jaringan.

Jaringan pribadi virtual memungkinkan sesi internet yang aman antara komputer jarak jauh dan server jaringan, seperti SSL.Tidak seperti SSL, VPN biasanya memerlukan perangkat keras dan perangkat lunakkhusus.Sebuah server gateway VPN umumnya melindungi server jaringan, dan komputer jarak jauh harus memiliki aplikasi klien VPN yang sesuai untuk membuat saluran yang aman (kadang-kadang disebut sebagai terowongan) untuk tujuan pertukaran data elektronik.*Internet Protocol Security* (IPSec) telah muncul sebagai standar protokol dominan untuk melaksanakan VPN. *Internet Protocol Security* dikembangkan oleh Internet Engineering Task Force (IETF), yang merupakan sekelompok ilmuwan dan ahli teknis lainnya yang memberikan dukungan pada masalah

teknis yang berhubungan dengan internet dan membantu mengembangkan standar internet. Tiga tujuan keamanan IPSec adalah untuk memberikan:

1. Mekanisme otentikasi, agarmemverifikasi secara andal atas identitas pengirim
2. Mekanisme integritas, agar menentukan secara andal bahwa data belum dimodifikasi selama transit dari sumbernya ke tujuannya
3. Mekanisme kerahasiaan, agar mengirimkan data yang dapat digunakan hanya oleh penerima yang dituju dan bukan oleh penyergap yang tidak sah[2]

Tujuan ini dicapai terutama melalui penggunaan enkripsi dan sertifikat digital.Dengan mengambil keuntungan dari infrastruktur internet yang ada di seluruh dunia, VPN yang digunakan dengan benar dapat memberikan penghematan biaya yang signifikan, efisiensi, dan manfaat lainnya bagi organisasi. Sebagai contoh:

- Pengguna jarak jauh dapat mengakses jaringan organisasi tanpa biaya panggilan telepon jarak jauh atau kebutuhan untuk organisasi membayar 800nomor.
- Koneksi situs ke situs tidak lagi memerlukan sirkit telepon sewa khusus yang mahal.
- Koneksi akses dapat dibuat hampir di mana saja di dunia.
- VPN dapat dibuat dan dibongkar dalam waktu yang relatif singkat.
- VPN dapat dirancang dengan enkripsi khusus yangkompleks dan kontrol otentikasi sehingga tampilan dan nuansa dari jaringan internal masing-masing organisasi disajikan kepada pengguna individu jarak jauh dan pengguna di masing-masing organisasi atau situs mitra komersial.
- VPN lebih aman dari aplikasi yang mengandalkan protokol lapisan soket yang aman untuk keamanan.[3]

Manfaat ini dapat diringkas dan dihitung dengan cara : "Menggunakan internet sebagai tulang punggung, VPN dapat menghubungkan semua kantor perusahaan dengan aman dan biaya yang efektif, telekomuter, pekerja *mobile*, pelanggan, mitra dan pemasok. Forester Research memperkirakan bahwa perusahaan dapat mencapai penghematan hingga 60 persen menggunakan internet berbasis VPN daripada jaringan pribadi dan bank modem perusahaan."[4]

Tetapi VPN juga memberikan sejumlah tantangan.Christopher King telah mengidentifikasi delapan tantangan tersebut.

1. Perangkat VPN harus memiliki metode yang disetujui bersama untuk mengamankan data (biasanya sertifikat digital). Tantangannya adalah bahwa saat ini bukan protokol standar untuk meminta, memvalidasi, dan menjamin persilangan sertifikat digital.
2. VPN harus dirancang agar memberikan ketersediaan yang tinggi kepada pengguna.
3. VPN harus dirancang untuk menanganiproduk komputasi enkripsi modern secara intensif selain memberikan pengolahan data kecepatan tinggi.
4. VPN harus dapat memindahkan dengan cepat volume tinggi data di antara pengguna melalui internet. Tantangannya adalah kadang-kadang dalam internet terdapat hambatan yang mencegah atau menunda data dari pencapaian tujuannya.
5. Jaringan internal organisasi harus dikonfigurasi agar perangkat gateway VPN tidak membahayakan mekanisme keamanan lain, seperti firewall.
6. Alamat dan jalur elektronik perangkat VPN harus hati-hati dirancang untuk memastikan bahwa urutan nomor alamat pribadi yang sama tidak ditugaskan untuk dua atau lebih jaringan yang berbeda.
7. Perangkat lunak penjual untuk VPN seringkali sulit untuk dilaksanakan dan dikelola.
8. Produk perangkat lunak VPN yang berbeda diberi label IPSec yang sesuai yang tidak harus bekerja sama.[5]

ADMINISTRASI KEAMANAN SISTEM

Administrasi keamanan sistem adalah proses di mana sebuah sistem informasi dilindungi dari akses yang tidak sah dan perusakan yang disengaja atau tidak disengaja atau perubahan. Bagaimana kontrol keamanan logis yang adadilaksanakan setelah sistem tersebut diimplementasikan sama pentingnya dengan desain kontrol keamanan logis. Sangat mungkin sebagian besar sistem yang ditemui di dunia nyata memiliki desain keamanan logis yang kurang optimal, sehingga mengangkat desakan memperkuat kontrol lain yang ada. Dalam beberapa kasus, kelemahan dalam desain keamanan logis pada sistem cukup dapat dikendalikan melalui pengembangan yang tepat dari kontrol keamanan logis lain yang ada. Dalam kasus lain, kelemahan tersebut tidak dapat dikendalikan secara memadai. Jika tidak, maka pengawasan kontrol dan prosedur harus dilaksanakan untuk mengidentifikasi potensi kerusakan sistem secara tepat waktu sampai sistem dapat dirancang ulang dan diprogram untuk mencegah kelemahan tersebut. Keamanan penting

terkait fungsi yang dilakukan oleh administrator keamanan sistem yaitu pembuatan ID pengguna dan persetujuan kemampuan akses sistem terkait, pengembangan parameter keamanan sistem, dan pengawasan sistem untuk membantu mencegah dan mendeteksi potensi terjadi penggunaan sistem yang tidak sah.

Ketika ID pengguna dibuat pertama kali oleh sistem, administrator keamanan sistem harus memberikan pengguna kemampuan akses yang sah saja dengan pemilik data, pemilik sistem, atau orang manajemen lain yang tepat. Administrator keamanan sistem hanya melakukan tindakan ini pada penerimaan otorisasi secaratertulis atau melalui pesan komunikasi elektronik yang aman.

Kadang-kadang teknisi penjual memasukkan ID pengguna sistem dan sandi awal selama pemasangan. Karena teknisi pemasangan biasanya tidak memiliki tujuan berkelanjutan untuk mengakses sistem setelah pemasangan selesai dan sukses, administrator keamanan sistem memastikan untuk merubah sandi ID pengguna sistem sehingga tidak ada satu orang pun yang mengetahuinya. Jika teknisi masih memerlukan akses untuk tujuan tertentu, administrator keamanan sistem membuat ID pengguna terpisah untuk teknisi tetapi hanya memberikan kemampuan akses yang dibutuhkan saja, tidak memberikan kemampuan akses administrasi sistem apapun.Tidak ada ID pengguna penjual luar yang diberikan kemampuan akses administrator keamanan sistem.

Manajer departemen harus bertanggung jawab untuk melatih pengguna untuk tidak berbagi atau membocorkan sandinya kepada siapa pun, menuliskannya, mencatat pada komputernya, menyimpan dalam berkas elektronik, atau melakukan tindakan lain yang secara poteinsial dapat mengakibatkan sandinya dibocorkan. Namun, semua daerah organisasi harus menekankan kepentingan pelatihan secara rahasia atas sandi untuk melindungi sistem informasi.Harus ada pernyataan kebijakan perusahaan dan standar khusus terkait kerahasiaan tersebut.(Lihat Bab 4 untuk pembahasan standar dan kebijakan keamanansistem informasi (SI)).Administrator keamanan sistem harus melaksanakan standar dan kebijakan tersebut.Auditor internal membantu memastikan bahwa kebijakan dan standar tersebut telah dilaksanakan dengan baik.Kebijakan dan standar harus dikomunikasikan kepada karyawan sebagai bagian dari program pelatihan karyawan baru.Selain itu, kartu pengingat petunjuk singkat dan pengingat periodik dalam buletin dan surat elektronik perusahaan harus disiapkan dan didistribusikan oleh departemen

administrasi keamanan sistem. Media komunikasi ini harus diperbarui pada secara teratur (misalnya kuartalan atau setengah tahunan).

Suatu prosedur harus dilaksanakan dimana kemampuan akses pengguna ditinjau secara periodik (misalnya, per tahun).Secara teori, manajemen harus melakukan tinjauan kemampuan akses periodik di daerah pengguna.Pada kenyataannya, pelaksanaan prosedur ini sangat sulit. Alasan utama adalah keterbatasan efektivitas tinjauan periodik, dalam kebanyakan kasus, personal manajemen dipanggil atas peninjauan dan persetujuan kemampuan akses sistem staf yang tidak mengerti apa arti semua kemampuan akses tersebut. Manajemen harus dididik dalam matriks keamanan akses sistem yang kompleks, tabel, fungsi khusus, hak, dan atribut yang mungkin pengguna gunakan dalam sistem.Pendidikan tersebut dapat dicapai melalui kursus pelatihan formal yang dilakukan oleh administrator keamanan sistem atau auditor SI yang akrab dengan keamanan akses sistem atas platform yang terkait.Semakin memperumit masalah adalah fakta ada banyaknya sistem komputer yang diakses oleh staf dalam suatu departemen. Sebagai contoh, ketika pengguna tertentu datang bekerja pada pagi hari, dia mungkin memeriksa kotak surat suaranya, mengakses ke jaringan dan memeriksa surat elektronik, memeriksa email internetnya, mengakses ke mainframe untuk memeriksa status laporan pekerjaan lain, dan kemudian mengakses beberapa aplikasi jaringan akses yang dilarang untuk melakukan berbagai tugas bisnis dan audit. Di akhir hari, pengguna mungkin telah mengakses 10 atau lebih sistem komputer yang dikelola secara independen.Pengguna lain dengan manajer yang sama juga mungkin mengakses 10 atau lebih sistem dalam sehari, tetapi mungkin tidak pada 10 sistem yang sama yang diakses oleh pengguna lain. Dalam departemen ada 15 atau 20 karyawan, sejumlah gabungan sistem yang berbeda yang diakses selama sehari 50 atau lebih.Dengan deminkian, pelatihan manajemen untuk memahami kemampuan akses sistem dalam semua sistem menjadi pekerjaan yang besar.

Haruskah manajer departemen diharapkan untuk mengerti dan menyetujui kemampuan akses sistem atas karyawan departemen pada semua sistem? Ini merupakan pertanyaan yang jawabannya akan berbeda oleh organisasi. Hal tersebut tergantung pada sifat sistem yang diakses, tingkat kontrol yang dilakukan oleh administrator keamanan sistem pada setiap sistem, oleh pemilik sistem dan/atau data pada setiap sistem, dan oleh pengguna akhir di manajemen. Ukuran organisasi dan budaya perusahaan juga akan memainkan peran dalam menentukan tingkat dimana akses berbagai sistem informasi dikelola dan diawasi. Jawaban realistis atas dilema ini adalah bahwa pengawasan

kemampuan akses sistem merupakan usaha luas organisasi bersama.Manajemen akhirnya bertanggung jawab atas kegiatan para stafnya.Namun, administrator keamanan sistem bertanggung jawab untuk melindungi sumber daya sistem dari akses yang tidak sah dan kerusakan.Oleh karena itu, mereka harus menyarankan manajemen mengenai mengapa kemampuan akses tertentu tidak harus diberikan. Auditor internal juga harus membantu pada keseluruhan proses dengan mengevaluasi sebab di balik kemampuan akses sistem yang diberikan, yaitu kemampuan dari administrator keamanan sistem sendiri.

Prosedur lain administrator keamanan sistem harus melakukan dengan segera menghilangkan ID pengguna atas pengguna yang dihentikan atau dialihkan. Prosedur harus ditetapkan agar perlunya manajer departemen dan/atau departemen sumber daya manusia memberitahukan semua administrator keamanan sistem yang ada ketika karyawan dihentikan atau dialihkan.Pemberitauan tersebut berlangsung selama satu hari atau kurang atas penghentian atau peralihan untuk mengurangi risiko tindakan yang tidak sah oleh karyawan yang dihentikan atau dialihkan sebelum akses sistemnya dicabut. Penggilan telepon merupakan cara tercepat untuk memberitahukan administrator keamanan sistem atas penghentian dan peralihan. Pemberitahuan telepon biasanya harus diikuti dengan memo tertulis.Pemberitahuan alternative berarti adalah email. Email sangat tepat waktu, dan jika sistem email dan ID pengguna berasal benar-benar aman, pesan email dapat berfungsi sebagai mekanisme otorisasi dokumen.

Sudi kasus 8.2 merupakan situasi di dunia nyata yang memberikan fakta bahwa kekuatan rancangan dan pengembangan atas kontrol keamanan logis dalam banyak organisasi bervariasi di seluruh spektrum dari sangat baik sampai hamper tidak ada. Karena pentingnya kontrol keaman logis pada seluruh lingkungan kontrol, sejumlah besar sutdi kasus telah disertakan.Dari banyak studi kasus ini, masalah telah dihindari atau setidaknya dikurangi oelh administrasi keamanan sistem yang efektif dan prosedur pengawasan.Banyak contoh dimana ID pengguna atas karyawan yang dihentikan dan dialihkan tidak dihilangkan menunjukkan bahwa ini merupakan salah satu dari kelemahan kontrol internal yang paling umum.Pada banyak kasus, kelemahan kontrol merupakan gabungan dari buruknya rancangan keamanan sistem dan pelaksanaan prosedur kontrol internal.

STUDI KASUS 8.2

Kelemahan Kontrol Pengolahan Cek

Selama audit operasi pengolahan cek masuk pada lembaga keuangan, berikut merupakan kelemahan kontrol yang ditemui :

- Fitur "jurnal audit"tidak diaktifkan. Platform yang dimaksud adalah IBM AS/400, dan manajer departemen juga merupakan administrator keamanan sistem. Jurnal audit AS/400 diatur untuk mencatat jenis utama kegiatan sistem seperti kegagalan otorisasi pengguna (misalnya gagal mengakses), operasi pemulihan sistem, operasi penghapusan, kegagalan program, penambahan, perubahan, dan penghapusan profil pengguna, dan kegiatan lainnya terkait keamana sistem.
- Agar menyediakan metode yang efektif dan aman atas peninjauan kegiatan sistem untuk transaksi yang sah, hal tersebut disarankan agar jurnal audit diaktifkan dan prosedur dilaksanakan dimana manajer departemen meninjau secara berkala dan menyetujui kegiatan yang ditunjukkan dalam jurnal. Hal itu juga disarankan agar manajer departemen bekerja dengan teknisi pendukung IBM untuk mengembangkan jadwal pengarsipan yang paling efektif dan efisien untuk pencatatan sehingga tidak akan memenuhi terlalu cepat dan dengan demikian menurunkan kinerja sistem.
- Tujuh pengguna memiliki kemampuan administrasi keamanan sistem ketika mereka seharusnya tidak memilikinya. Salah satunya digunakan oleh penjual yang menginstal aplikasi bisnis, enam lainnya merupakan ID pengguna latihan yang digunakan untuk menjalankan tutorial sistem operator. Keberadaan ID pengguna ini meningkatkan risiko atas akses yang tidak sah.
- Sandi awal lima dari enam ID pengguna sistem asli tidak diubah sejak sistem pertama kali dipasang empat tahun yang lalu. Karena sandi awal didokumentasikan dengan baik dalam buku panduan penjual, akan meningkatkan risiko akses yang tidak sah dan merubah pengaturan keamanan. Ini akan menjadi lebih baik jika penjual telah merancang dan memprogram sistem untuk meminta ID pengguna dari semua pengguna, termasuk administrator keamanan sistem, untuk mengubah sandi awal mereka selama awal akses. Dianjurkan agar administrator keamanan sistem mengirimkan permintaan ini kepada penjual untuk mempertimbangkan pemrograman dalam rilis yang akan datangatas perangkat lunak. Jika pengguna tidak menginformasikan penjualbahwa mereka ingin fitur keamanan sistem yang lebih baik, penjualkecil kemungkinannya mengeluarkan sumber daya untuk menyediakan mereka.
- Tiga kelemaha kontrol akses sistem yang diidentifikasi :

1. Pengguna dibolehkan memiliki sesi akses yang bersamaan (contoh, mengakses pada lebih dari satu komputer pada saat yang sama).
2. Kontrol akses normal tidak diperlukan atas pengguna jarak jauh yang mengakses sistem melalui modem. Pengguna jarak jauh ini biasanya penjual aplikasi.
3. Fiturs sesi habis waktu otomatis tersedia tetapi tidak diaktifkan.

Untuk memberikan perlindungan yang tinggi terhadap akses yang tidak sah, disarankan agar sesi akses dibatasi hanya pada satu komputer pada satu waktu, pengaturan akses jarak jauh diubah ke permintaan akses pada semua pengguna, yaitu mengaksesnya dari jarak jauh, dan sesi habis waktu otomatis diatur 10 menit (5 menit lebih diinginkan, tetapi 10 menit telah disetujui untuk alasan efisiensi dan efektivitas operasional.

Selama audit proses ATM, kecukupan kontrol keamanan logis dari tiga aplikasi yang berbeda, yang masing-masing melayani aspek yang berbeda dari proses *back office* ATM, dinilai. Aplikasi tersebut diberikan oleh penjual layanan pergantian ATM lokal.Sistem keamanan dikelola oleh manajer departemen ATM di lembaga keuangan.

Aplikasi Penyesuaian Permintaan ATM Penjual

Beberapa kelemahan desain dan kelemahan administrasi keamanan sistem teridentifikasi dalam aplikasi ini, dimana mengakibatkan peningkatan risiko akses yang tidak sah.Kelemahan dalam desain adalah sandi bisa sesingkat dua karakter, administrator keamanan sistem bisa melihat sandi pengguna dari dalam aplikasi, dan kurangnya fitur kadaluarsa sandi. Kelemahan administrasi sistem keamanan yaitu dua karyawan yang telah dipindahkan ke area lain dari perusahaan masih memiliki ID pengguna yang valid pada sistem; satu pengguna memiliki tiga ID pengguna berbeda yang sah, salah satunya memiliki kemampuan akses administrator keamanan sistem meskipun akses tersebut adalah bukan bagian dari tugas normalnya, dan satu ID pengguna yang valid ada pada karyawan yang telah dihentikan beberapa bulan sebelumnya.

Aplikasi Penggantian Kartu/PIN ATM Penjual

Seperti aplikasi sebelumnya, kelemahan ditemukan baik dalam desain keamanan sistem dan administrasi.Masalah desain adalah sandi bisa sesingkat empat karakter dan fitur kadaluarsa sandi tidak tersedia. Kelemahan kontrol administrasi keamanan sistem yaituterjadinyalimapengguna diberikan kemampuan akses sistem, yang memungkinkan mereka membersihkan berkas catatankejadian audit yang berhubungan dengan keamanan sistem dan melakukan fungsi desain layar aplikasi. Selain itu, disket sistem yang asli disimpan di buku petunjuk dokumentasi pengguna, bukan di lokasi yang terkunci.

Aplikasi Hotcarding ATM Penjual

Kelemahan dalam desain keamanan sistem dan kelemahan administrasi juga terlihat dalam sistem ini.Kelemahan dalam desain yaitu sandi singkat dengan nol karakter dan kurangnya fitur kadaluarsa sandi.Kelemahan kontrol yang bisa dihindari dengan prosedur administrasi keamanan sistem yang tepat yaitusalah satu pengguna memiliki kemampuan akses administrator keamanan sistem yang tidak diperlukan sebagai bagian dari tugas normalnya, administrator keamanan sistem memiliki pengaturan parameter sesi waktu

habis selama 20 menit bukannya 5 menit seperti pengguna lain, dan semua ID pengguna diberi nama menurut posisi departemen bukan nama pengguna. Kelemahan kontrol terakhir ini secara operasional bisa diterapkan asalkan nama posisi unik dan sandi tidak dimiliki oleh beberapa pengguna. Rupanya praktik menetapkan namapengguna sebenarnya pada ID pengguna memberikan jejak audit yang lebih baik.

Ringkasan dari Aplikasi ATM Penjual

Tentu saja, dari jumlah dan jenis kelamahan desain yang dijelaskan dari masing-masing tiga aplikasi, keamanan sistem bukanlah pertimbangan utama dalam pengembangan tahap desain. Departemen ATM menambah kelemahan dalam desain keamanan sistem dengan tidak menerapkan prosedur administrasi keamanan sistem yang memadai.

Dianjurkan agar manajemen Departemen ATM mengirim surat kepada penjual layanan pergantian ATM, meminta agar setiap kelemahan desain keamanan yang teridentifikasi dikoreksi dalam keluaranaplikasi ATM mendatang. Juga direkomendasikan agar manajemen Departemen ATM mengatasi kelemahan pengendalian yang teridentifikasi dan menerapkan prosedur untuk membantu memastikan agar kelemahan pengendalian serupa tidak terjadi lagi.

Daftar Pustaka

1. See the discussion and examples on backup system security administrators in Chapter7 for some examples of why their activities need to be limited.
2. Pete Loshin, "IP: The Next Generation," *Information Security* (October 1998): 21.
3. The technical reason is that VPN security occurs at a lower level in the ISO (International Organization for Standardization) OSI (Open Systems Interconnect) model.
   The ISO model has seven layers that are commonly referred to as a "stack." Startingfrom highest to lowest, the layers are: Application, Presentation, Session, Transport,Network, Data Link, Physical. VPN security occurs at the network layer while SSLsecurity occurs at the transport layer.
4. Christopher M. King, CISSP, "The 8 Hurdles to VPN Deployment," *Information Security* (March 1999): 23.

5. Ibid.
6. "Lax Security Leads to Wire Transfer Loss," *Bank Fraud, Bulletin of Fraud and RiskManagement* (April 1996): 2–3.
7. "Russian Computer Expert Charged with Citibank Security Breach," *Bloomberg NewsService* (August 21, 1995).
8. "Citibank Hit by Fraudulent Transfers," *Infosecurity News* (November/December1995): 12.
9. "Former ABN Amro Employee Charged with Embezzling $1.9 Million," *BloombergNews Service* (May 31, 1995).
10. "Office Manager Pleads Guilty to Massive Embezzlement," *The Credit Union Accountant*(September 13, 1993): 5.
11. Martha Woodcock, "Costly Crimes Could Be Thwarted by Simple Measures," *CreditUnion Times* (March 15, 1995): 19.