Mengamankan Sistem Informasi

Dalam menjalankan bisnis saat ini, maka yang perlu dilakukan dan menjadi prioritas utama adalah membuat keamanan dan mengendalikan Sistem Informasi. Keamanan mengacu pada kebijakan, prosedur, dan langkah-langkah teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan, pencurian, atau: kerusakan fisik untuk sistem informasi. Kontrol adalah metode, kebijakan, dan prosedur organisasi yang menjamin keamanan aset organisasi; akurasi dan keandalan catatan nya; dan kepatuhan operasional untuk standar manajemen.

MENGAPA SISTEM RENTAN

 Ketika sejumlah besar data yang disimpan dalam bentuk elektronik, mereka rentan terhadap banyak jenis ancaman daripada ketika mereka ada dalam bentuk manual. Melalui jaringan komunikasi, sistem informasi di lokasi yang berbeda saling berhubungan. Potensi akses yang tidak sah, penyalahgunaan, atau penipuan tidak terbatas pada satu lokasi tetapi dapat terjadi pada setiap titik akses dalam jaringan.

Sistem kerusakan jika perangkat keras komputer rusak, tidak dikonfigurasi dengan benar, atau rusak oleh penggunaan yang tidak benar atau tindakan kriminal. Kesalahan dalam Program- ming, instalasi yang tidak tepat, atau perubahan yang tidak sah menyebabkan perangkat lunak komputer untuk gagal. gangguan listrik, banjir, kebakaran, atau bencana alam lainnya juga dapat mengganggu sistem komputer.

**Kerentanan Internet**

jaringan publik yang besar, seperti Internet, lebih rentan daripada jaringan internal yang karena mereka hampir terbuka untuk siapa saja. Internet adalah begitu besar sehingga ketika pelanggaran terjadi, mereka dapat memiliki dampak sangat besar luas. Ketika internet menjadi bagian dari jaringan perusahaan, sistem informasi organisasi bahkan lebih rentan terhadap tindakan dari pihak luar.

Komputer yang selalu terhubung ke Internet dengan modem kabel atau digital subscriber line (DSL) garis yang lebih terbuka untuk penetrasi oleh pihak luar karena mereka menggunakan alamat Internet tetap di mana mereka dapat dengan mudah diidentifikasi. (Dengan layanan dial-up, alamat Internet sementara ditugaskan untuk setiap sesi.) Sebuah alamat Internet tetap menciptakan target tetap untuk hacker.

layanan telepon berbasis teknologi Internet (lihat Bab 7) lebih rentan daripada jaringan suara beralih jika tidak menjalankan melalui jaringan pribadi yang aman. Kebanyakan Voice over IP (VoIP) lalu lintas melalui Internet publik tidak dienkripsi, sehingga siapapun dengan jaringan dapat mendengarkan percakapan. Hacker dapat mencegat percakapan atau menutup layanan suara dengan server banjir mendukung VoIP dengan lalu lintas palsu.

**Tantangan Keamanan Wireless**

Apakah aman untuk masuk ke jaringan nirkabel di bandara, perpustakaan, atau lokasi umum lainnya? Hal ini tergantung pada seberapa waspada Anda. Bahkan jaringan nirkabel di rumah Anda rentan karena pita frekuensi radio yang mudah untuk memindai. jaringan Bluetooth dan Wi-Fi rentan terhadap hacking oleh penyadap. Meskipun jangkauan jaringan Wi-Fi hanya beberapa ratus kaki, dapat diperpanjang sampai dengan seperempat mil menggunakan antena eksternal. jaringan area lokal (LAN) menggunakan standar 802.11 dapat dengan mudah ditembus oleh siders out berbekal laptop, kartu wireless, antena eksternal, dan hacking gudang soft. Hacker menggunakan alat ini untuk mendeteksi jaringan yang tidak dilindungi, memonitor lalu lintas jaringan, dan, dalam beberapa kasus, mendapatkan akses ke Internet atau ke jaringan perusahaan. teknologi transmisi Wi-Fi dirancang untuk memudahkan stasiun untuk menemukan dan mendengar satu sama lain. Service set identifier (SSID) mengidentifikasi titik-titik akses di jaringan Wi-Fi yang disiarkan beberapa kali dan dapat diambil cukup mudah dengan program sniffer penyusup. di mana penyadap mengawasi melalui bangunan atau parkir di luar dan mencoba untuk memotong lalu lintas jaringan nirkabel

**SOFTWARE JAHAT: VIRUS, worm, trojan horse, DAN SPYWARE**

program perangkat lunak berbahaya yang disebut sebagai malware dan meliputi berbagai ancaman, seperti virus komputer, worm, dan trojan horse. Sebuah virus komputer adalah sebuah program perangkat lunak jahat yang menempel pada program perangkat lunak atau file data lainnya dalam rangka untuk dieksekusi, biasanya tanpa sepengetahuan pengguna atau izin. Kebanyakan virus komputer memberikan “payload.” Payload mungkin relatif jinak, seperti petunjuk untuk menampilkan pesan atau gambar, atau mungkin sangat merusak-merusak program atau data, menyumbat memori komputer, memformat hard drive komputer, atau program menyebabkan untuk menjalankan benar. Virus biasanya menyebar dari komputer ke komputer ketika manusia mengambil tindakan, seperti mengirim lampiran e-mail atau menyalin file yang terinfeksi.

Paling serangan baru-baru datang dari cacing, yang merupakan program komputer independen yang menyalin diri dari satu komputer ke komputer ers comput- lain melalui jaringan. (Tidak seperti virus, mereka dapat beroperasi sendiri tanpa melampirkan ke file program komputer lain dan kurang mengandalkan perilaku manusia dalam rangka untuk menyebar dari komputer ke komputer. Hal ini menjelaskan mengapa cacing komputer menyebar jauh lebih cepat daripada virus komputer.) Worms menghancurkan data dan program serta mengganggu atau bahkan menghentikan pengoperasian jaringan komputer.

Worm dan virus sering menyebar melalui Internet dari file dari perangkat lunak download, dari file yang melekat transmisi ke e-mail, atau dari pesan e-mail dikompromikan atau pesan instan. Virus juga telah menyerang sistem informasi terkomputerisasi dari “terinfeksi” disk atau mesin yang terinfeksi. E-mail worm saat ini yang paling bermasalah. Dan unduh file dari Web melalui Wi-Fi atau jaringan seluler. Saat ini ada lebih dari 200 virus dan worm yang menargetkan ponsel, seperti Cabir, Commwarrior, Frontal.A, dan Ikee.B. Frontal.A menginstal file rusak yang menyebabkan kegagalan telepon dan mencegah pengguna dari rebooting, sementara Ikee.B mengubah iPhone yang di-jailbreak menjadi perangkat yang dikontrol botnet. Virus perangkat seluler menimbulkan ancaman serius terhadap komputasi perusahaan karena begitu banyak perangkat nirkabel sekarang terhubung ke sistem informasi perusahaan. Aplikasi Web 2.0, seperti blog, wiki, dan situs jejaring sosial seperti Facebook dan MySpace, telah muncul sebagai saluran baru untuk malware atau spyware. Aplikasi ini memungkinkan pengguna untuk memposting kode perangkat lunak sebagai bagian dari konten yang diizinkan, dan kode tersebut dapat diluncurkan secara otomatis segera setelah halaman Web dilihat. Studi kasus pembukaan bab menggambarkan saluran lain untuk malware yang menargetkan Facebook. Pada September 2010, peretas mengeksploitasi celah keamanan Twitter untuk mengirim pengguna ke situs pornografi Jepang dan secara otomatis menghasilkan pesan dari akun lain (Coopes, 2010).

Sebuah **Trojan horse** adalah program software yang tampaknya jinak tapi kemudian melakukan sesuatu yang lain dari yang diharapkan, seperti Zeus Trojan dijelaskan dalam kasus bab-pembukaan. Trojan horse tidak sendiri virus karena tidak meniru, tetapi sering merupakan cara untuk virus atau kode berbahaya lainnya untuk intro- diproduksi ke dalam sistem komputer. Kuda Trojan jangka didasarkan pada kuda kayu yang besar digunakan oleh orang Yunani untuk mengelabui Trojan untuk membuka gerbang ke kota mereka dibentengi selama Perang Troya. Setelah di dalam tembok kota, Diers sol Yunani tersembunyi di kuda mengungkapkan diri mereka sendiri dan merebut kota.

Saat ini, **serangan injeksi SQL** adalah ancaman malware terbesar. Serangan injeksi SQL memanfaatkan kerentanan dalam perangkat lunak aplikasi Web yang dikodekan dengan buruk untuk memperkenalkan kode program jahat ke dalam sistem dan jaringan perusahaan. Kerentanan ini terjadi ketika aplikasi Web gagal untuk memvalidasi atau memfilter data yang dimasukkan oleh pengguna pada halaman Web, yang mungkin terjadi ketika memesan sesuatu secara online. Seorang penyerang menggunakan kesalahan validasi input ini untuk mengirim permintaan SQL palsu ke basis data yang mendasari untuk mengakses database, menanam kode berbahaya, atau mengakses sistem lain di jaringan. Aplikasi Web besar memiliki ratusan tempat untuk memasukkan data pengguna, yang masing-masing menciptakan peluang untuk serangan injeksi SQL.

 Sebagian besar aplikasi yang berhadapan dengan Web diyakini memiliki kerentanan injeksi SQL, dan alat-alat tersedia untuk peretas untuk memeriksa aplikasi Web untuk kerentanan ini. Alat tersebut dapat menemukan bidang entri data pada formulir halaman Web, memasukkan data ke dalamnya, dan memeriksa respons untuk melihat apakah menunjukkan kerentanan terhadap injeksi SQL.

 Beberapa jenis spyware juga bertindak sebagai perangkat lunak berbahaya. Program-program kecil ini memasang diri mereka secara diam-diam di komputer untuk memonitor aktivitas pengguna internet dan melayani iklan. Ribuan bentuk spyware telah didokumentasikan.

 Banyak pengguna menemukan spyware semacam itu menjengkelkan dan beberapa kritik khawatir tentang itu

pelanggaran privasi pengguna komputer. Beberapa bentuk spyware terutama jahat. Keylogger merekam setiap keystroke yang dibuat pada komputer untuk mencuri nomor seri untuk perangkat lunak, untuk meluncurkan serangan Internet, untuk mendapatkan akses ke akun email, untuk mendapatkan kata sandi untuk melindungi sistem komputer, atau untuk mengambil informasi

pribadi seperti nomor kartu kredit. Program spyware lainnya mereset halaman muka browser web, mengarahkan permintaan pencarian, atau memperlambat kinerja dengan mengambil terlalu banyak memori. Trojan Zeus yang dijelaskan dalam kasus pembukaan bab menggunakan keylogging untuk mencuri informasi keuangan.

HACKER DAN KEJAHATAN KOMPUTER

Seorang peretas adalah individu yang berniat mendapatkan akses tidak sah ke sistem komputer. Dalam komunitas hacking, istilah cracker biasanya digunakan untuk menunjukkan hacker dengan maksud kriminal, meskipun dalam pers publik, istilah hacker dan cracker digunakan secara bergantian. Peretas dan cracker mendapatkan akses tidak wajar dengan mencari kelemahan dalam perlindungan keamanan yang digunakan oleh situs Web dan sistem komputer, sering memanfaatkan berbagai fitur Internet yang menjadikannya sistem terbuka yang mudah digunakan.

Aktivitas peretas telah meluas melampaui gangguan sistem semata untuk memasukkan pencurian barang dan informasi, serta kerusakan sistem dan cybervandalisme, gangguan yang disengaja, perusakan, atau bahkan perusakan situs Web atau sistem informasi perusahaan. Misalnya, cybervandals telah mengubah banyak situs "kelompok" MySpace, yang didedikasikan untuk kepentingan seperti pembuatan bir rumah atau kesejahteraan hewan, ke dalam dinding cyber-grafiti, penuh dengan komentar dan foto yang menyinggung.

**Spoofing dan Sniffing**

Hacker berusaha menyembunyikan identitas mereka yang sebenarnya, sering menipu, atau menyesatkan, dengan menggunakan alamat e-mail palsu atau menyamar sebagai orang lain. Spoofing juga mungkin melibatkan pengalihan tautan Web ke alamat yang berbeda dari yang dimaksudkan, dengan situs yang menyamar sebagai tujuan yang dimaksud. Sebagai contoh, jika peretas mengarahkan pelanggan ke situs Web palsu yang terlihat hampir persis seperti situs yang sebenarnya, mereka kemudian dapat mengumpulkan dan memproses pesanan, secara efektif mencuri bisnis serta informasi pelanggan yang sensitif dari situs yang sebenarnya. Kami memberikan lebih banyak detail tentang bentuk spoofing lainnya dalam diskusi kami tentang kejahatan komputer.

 Sniffer adalah sejenis program penguping yang memantau informasi

bepergian melalui jaringan. Ketika digunakan secara sah, sniffer membantu mengidentifikasi titik-titik masalah jaringan potensial atau aktivitas kriminal di jaringan, tetapi ketika digunakan untuk tujuan kriminal, mereka dapat merusak dan sangat sulit untuk dideteksi. Sniffer memungkinkan peretas mencuri informasi eksklusif dari mana saja di jaringan, termasuk pesan e-mail, file perusahaan, dan laporan rahasia.

**Penolakan Serangan Terhadap layanan**

Dalam serangan denial-of-service (DoS), peretas membanjiri server jaringan atau server Web dengan ribuan komunikasi palsu atau permintaan layanan untuk merusak jaringan. Jaringan menerima begitu banyak pertanyaan sehingga tidak dapat mengikuti mereka dan karena itu tidak tersedia untuk melayani permintaan yang sah. Serangan denial-of-service (DDoS) terdistribusi menggunakan banyak komputer untuk membanjiri dan membanjiri jaringan dari berbagai titik peluncuran.

Sebagai contoh, selama 2009 protes pemilu Iran, aktivis asing berusaha untuk membantu oposisi terlibat dalam serangan DDoS terhadap Iran pemerin- ment. Situs Web resmi Iran pemerintah (ahmadinejad.ir) telah diberikan tidak dapat diakses pada beberapa kesempatan.

Meskipun serangan DoS tidak merusak daerah informasi atau akses terbatas dari sistem informasi perusahaan, mereka sering menyebabkan situs Web untuk menutup, sehingga mustahil untuk pengguna yang sah untuk mengakses situs ini. Untuk situs e-commerce sibuk, serangan ini mahal; sementara situs dimatikan, pelanggan tidak dapat melakukan pembelian. Terutama rentan adalah usaha kecil dan menengah yang jaringan cenderung kurang dilindungi dibandingkan ransum corpo- besar.

Pelaku serangan DoS sering menggunakan ribuan “zombie” PC yang terinfeksi dengan perangkat lunak berbahaya tanpa sepengetahuan pemiliknya dan disusun dalam sebuah botnet. Hacker membuat botnet tersebut dengan menginfeksi komputer orang lain dengan bot malware yang membuka pintu belakang melalui mana seorang penyerang bisa memberikan instruksi. komputer yang terinfeksi kemudian menjadi budak, atau zombie, melayani master komputer milik orang lain. Sekali hacker menginfeksi cukup komputer, atau dia dapat menggunakan sumber daya mengumpulkan botnet untuk memulai serangan DDos, kampanye phishing, atau tidak diminta “spam” e-mail.

Jumlah komputer yang merupakan bagian dari botnet adalah berbagai diperkirakan 6-24 juta dengan ribuan botnet beroperasi di seluruh dunia. Serangan botnet terbesar pada 2010 adalah botnet Mariposa, yang dimulai di Spanyol dan menyebar ke seluruh dunia. Mariposa telah terinfeksi dan menguasai sekitar 12,7 juta komputer dalam upaya untuk mencuri nomor kartu kredit dan password online banking. Lebih dari separuh perusahaan Fortune 1000, 40 bank-bank besar, dan banyak instansi pemerintah terinfeksi-dan tidak tahu itu.

 Studi kasus pada akhir bab menggambarkan beberapa gelombang serangan DDoS yang menjaring sejumlah situs web lembaga pemerintah dan organisasi lain di Korea Selatan dan Amerika Serikat pada bulan Juli 2009. Penyerang menggunakan botnet yang mengontrol lebih dari 65.000 komputer, dan mampu untuk melumpuhkan beberapa situs ini selama beberapa hari. Sebagian besar botnet berasal dari China, dan Korea Utara. Serangan botnet yang diduga berasal dari Rusia bertanggung jawab untuk melumpuhkan situs Web pemerintah Estonia pada April 2007 dan pemerintah Georgia pada Juli 2008.

**Kejahatan Komputer**

Sebagian besar aktivitas peretas adalah pelanggaran kriminal, dan kerentanan sistem yang baru saja kami jelaskan menjadikannya target untuk jenis kejahatan komputer lainnya juga. Misalnya, pada awal Juli 2009, agen federal AS menangkap Sergey Aleynikov, seorang programmer komputer di firma perbankan investasi Goldman Sachs, karena mencuri program komputer eksklusif yang digunakan untuk membuat perdagangan cepat yang menguntungkan di pasar keuangan. Perangkat lunak ini membawa Goldman jutaan dolar keuntungan per tahun dan, di tangan yang salah, dapat digunakan untuk memanipulasi pasar keuangan dengan cara yang tidak adil. Kejahatan komputer didefinisikan oleh Departemen Kehakiman AS sebagai "setiap pelanggaran hukum pidana yang melibatkan pengetahuan tentang teknologi komputer untuk perbuatan mereka, investigasi, atau penuntutan." Tabel 8-2 memberikan contoh komputer sebagai target kejahatan dan sebagai alat kejahatan.

 Tidak ada yang tahu besarnya masalah kejahatan computer, berapa banyak sistem yang diserang, berapa banyak orang yang terlibat dalam praktik, atau kerusakan ekonomi total. Menurut Survei Kejahatan dan Keamanan Komputer CSI 2009 dari 500 perusahaan, rata-rata kerugian tahunan peserta dari kejahatan komputer dan serangan keamanan mendekati $ 234.000 (Computer Security Institute, 2009). Banyak perusahaan yang enggan melaporkan kejahatan komputer karena kejahatan itu mungkin melibatkan karyawan, atau perusahaan khawatir bahwa mempublikasikan kerentanannya akan merusak reputasinya. Jenis kejahatan komputer yang paling merusak secara ekonomi adalah serangan DoS, datangnya virus baru, pencurian layanan, dan gangguan sistem komputer.

**Pencurian identitas**

Dengan pertumbuhan internet dan perdagangan elektronik, pencurian identitas telah menjadi sangat mengganggu. Pencurian identitas adalah kejahatan di mana seorang penipu memperoleh potongan kunci informasi pribadi, seperti nomor jaminan sosial identifikasi, nomor SIM, atau nomor kartu kredit, untuk menyamar sebagai orang lain. Informasi yang dapat digunakan untuk memperoleh kredit, barang, atau jasa atas nama korban atau untuk memberikan pencuri dengan mandat palsu. Menurut Javelin Strategy dan Penelitian, kerugian dari pencurian identitas naik ke

$ 54 miliar pada tahun 2009, dan lebih dari 11 juta orang dewasa AS adalah korban penipuan identitas (Javelin Strategy & Research, 2010).

Mengidentifikasi pencurian telah berkembang di Internet, dengan kartu kredit file target utama dari situs Web hacker. Selain itu, e-commerce adalah sumber indah dari pelanggan pribadi informasi-nama, alamat, dan nomor telepon. Berbekal informasi ini, penjahat dapat mengasumsikan identitas baru dan membangun kredit baru untuk tujuan mereka sendiri.

Salah satu taktik semakin populer adalah bentuk spoofing disebut phishing. phishingmelibatkan pengaturansitus palsu Web atau mengirim e-mail atau pesan teks yang terlihat seperti orang-orang dari bisnis yang sah untuk meminta pengguna untuk data pribadi yang bersifat rahasia. Pesan menginstruksikan penerima untuk memperbarui atau mengkonfirmasi catatan dengan memberikan nomor jaminan sosial, bank dan informasi kartu kredit, dan lainnya data rahasia baik dengan menanggapi pesan e-mail, dengan memasukkan informasi di situs Web palsu, atau dengan menelepon telepon jumlah. EBay, PayPal, Amazon.com, Walmart, dan berbagai bank, adalah salah satu perusahaan top palsu.

teknik phishing baru yang disebut kembar jahat dan pharming lebih sulit untuk dideteksi. kembar jahat adalah jaringan nirkabel yang berpura-pura menawarkan dipercaya koneksi Wi-Fi ke Internet, seperti di lounge bandara, hotel, atau toko-toko kopi. Jaringan palsu terlihat identik dengan jaringan publik yang sah. Penipu mencoba untuk menangkap password atau nomor kartu kredit pengguna tanpa disadari yang log on ke jaringan.

**pharming** mengarahkan pengguna ke halaman Web palsu, bahkan ketika jenis individu alamat halaman Web yang benar ke dalam browser-nya. Hal ini dimungkinkan jika pharming pelaku mendapatkan akses ke informasi alamat Internet yang disimpan oleh penyedia layanan Internet untuk mempercepat browsing Web dan perusahaan ISP telah cacat perangkat lunak pada server mereka yang memungkinkan penipu untuk hack dan mengubah alamat mereka.

Dalam contoh terbesar dari pencurian identitas sampai saat ini, Alberto Gonzalez dari Miami dan dua Rusia co-konspirator menembus sistem perusahaan dari TJX Corporation, Hannaford Brothers 7-Eleven, dan pengecer besar lainnya, mencuri lebih dari 160 juta nomor kartu kredit dan debit antara 2005 dan 2008. kelompok awalnya ditanam “sniffer” program dalam jaringan komputer perusahaan-perusahaan yang menangkap data kartu seperti mereka yang sedang ditransmisikan antara sistem komputer. Mereka kemudian beralih ke serangan injeksi SQL, yang kita diperkenalkan di awal bab ini, untuk menembus database perusahaan. Pada bulan Maret 2010, Gonzalez dijatuhi hukuman 20 tahun penjara. TJX saja menghabiskan lebih dari $ 200 juta untuk menangani pencurian data, termasuk permukiman hukum.

Kongres AS membahas ancaman kejahatan komputer pada tahun 1986 dengan Penipuan dan Penyalahgunaan Komputer Act. Tindakan ini membuatnya ilegal untuk mengakses sistem komputer tanpa otorisasi.

 dan serangan hacker yang menonaktifkan situs Web kejahatan federal. undang-undang AS, seperti penyadapan UU, UU Kawat Penipuan, Undang-Undang Spionase Ekonomi, Electronic Communications Privacy Act, Ancaman E-mail dan Pelecehan Act, dan Anak UU Pornografi, mencakup kejahatan komputer yang melibatkan mencegat komunikasi elektronik, menggunakan komunikasi elektronik untuk menipu, mencuri rahasia dagang, ilegal mengakses disimpan komunikasi elektronik, menggunakan e-mail untuk ancaman atau pelecehan, dan transmisi atau memiliki pornografi anak.

**klik Penipuan**

Ketika Anda mengklik pada iklan yang ditampilkan oleh mesin pencari, pengiklan biasanya membayar biaya untuk setiap klik, yang seharusnya mengarahkan calon pembeli untuk produk-produknya. Klik penipuan terjadi ketika seorang individu atau program komputer fraudu- lently mengklik iklan online tanpa niat belajar lebih banyak tentang pengiklan atau melakukan pembelian. Klik penipuan telah menjadi masalah serius di Google dan situs web lainnya yang menampilkan bayar per-klik iklan online.

Beberapa perusahaan menyewa pihak ketiga (biasanya dari negara-upah rendah) untuk menipu mengklik iklan pesaing untuk melemahkan mereka dengan menaikkan biaya pemasaran mereka. Klik penipuan juga dapat dilakukan dengan program perangkat lunak melakukan klik, dan botnet yang sering digunakan untuk tujuan ini. mesin pencari seperti Google upaya untuk memantau penipuan klik tapi enggan untuk mempublikasikan usaha mereka untuk menangani masalah ini.

**Ancaman global: Cyberterrorism dan Cyber ​​perang tarif**

Kegiatan cybercriminal kami telah dijelaskan-meluncurkan malware, serangan layanan denial-of-, dan phishing probe-yang tanpa batas. perusahaan keamanan komputer Sophos melaporkan bahwa 42 persen dari malware itu diidentifikasi pada awal 2010 berasal dari Amerika Serikat, sedangkan 11 persen berasal dari Cina, dan 6 persen dari Rusia (Sophos, 2010). Sifat global internet membuat pos- jawab untuk penjahat cyber untuk mengoperasikan-dan merugikan-mana saja di dunia.

Perhatian yang dipelajari bahwa kerentanan Internet atau jaringan lain membuat jaringan digital target mudah bagi serangan digital oleh teroris, layanan intelijen asing, atau kelompok lain berusaha untuk menciptakan gangguan yang luas dan membahayakan. cyberattacks seperti mungkin menargetkan perangkat lunak yang berjalan grid listrik listrik, sistem kontrol lalu lintas udara, atau jaringan dari bank-bank besar dan lembaga keuangan. Setidaknya 20 negara, termasuk China, diyakini mengembangkan kemampuan cyberwarfare ofensif dan defensif. The chapter- berakhir studi kasus membahas masalah ini secara lebih rinci.

ANCAMAN INTERNAL: KARYAWAN

Kita cenderung berpikir ancaman keamanan untuk bisnis berasal dari luar lisasi-lembaga yang. Bahkan, orang dalam perusahaan menimbulkan masalah keamanan serius. Karyawan memiliki akses ke informasi rahasia, dan di hadapan prosedur keamanan internal ceroboh, mereka sering mampu menjelajah seluruh sistem organisasi tanpa meninggalkan jejak.

Studi telah menemukan bahwa kurangnya pengguna pengetahuan adalah penyebab tunggal terbesar dari pelanggaran keamanan jaringan. Banyak karyawan lupa password mereka untuk mengakses sistem komputer atau mengizinkan rekan kerja untuk menggunakannya, yang kompromi sistem.

penyusup berbahaya mencari akses sistem kadang-kadang menipu karyawan untuk mengungkapkan password mereka dengan berpura-pura menjadi anggota sah dari perusahaan yang membutuhkan informasi. Praktek ini disebut social engineering.

Kedua pengguna akhir dan spesialis sistem informasi juga merupakan sumber utama dari kesalahan yang diperkenalkan ke dalam sistem informasi. pengguna akhir memperkenalkan kesalahan dengan

memasukkan data yang salah atau dengan tidak mengikuti petunjuk yang tepat untuk pengolahan data dan menggunakan peralatan komputer. spesialis sistem informasi dapat membuat kesalahan perangkat lunak saat mereka merancang dan mengembangkan perangkat lunak baru atau mempertahankan program yang ada.

**KERENTANAN PERANGKAT LUNAK**

kesalahan perangkat lunak menimbulkan ancaman konstan untuk sistem informasi, menyebabkan kerugian yang tak terhitung produktivitas. Tumbuh kompleksitas dan ukuran program perangkat lunak, cou- memohon dengan tuntutan untuk pengiriman tepat waktu ke pasar, telah memberikan kontribusi untuk peningkatan kelemahan perangkat lunak atau kerentanan Misalnya, kesalahan perangkat lunak yang berhubungan dengan database dicegah jutaan JP Morgan Chase ritel dan usaha kecil pelanggan mengakses rekening bank online mereka selama dua hari pada September 2010 (Dash, 2010).

Masalah utama dengan perangkat lunak adalah adanya bug tersembunyi atau cacat kode program. Penelitian telah menunjukkan bahwa hampir tidak mungkin untuk menghilangkan semua bug dari program besar. Sumber utama bug adalah kompleksitas deci- kode sion pembuatan. Sebuah program yang relatif kecil dari beberapa ratus baris akan con- tain puluhan keputusan yang mengarah ke ratusan atau bahkan ribuan jalan yang berbeda. program penting dalam kebanyakan perusahaan biasanya jauh lebih besar, contain- ing puluhan ribu atau bahkan jutaan baris kode, masing-masing dengan kali pilihan dan jalur dari program yang lebih kecil.

Nol cacat tidak dapat dicapai dalam program yang lebih besar. pengujian lengkap hanya tidak mungkin. Sepenuhnya menguji program yang berisi ribuan pilihan dan jutaan jalur akan membutuhkan ribuan tahun. Bahkan dengan pengujian yang ketat, Anda tidak akan tahu pasti bahwa software adalah diandalkan sampai produk membuktikan diri setelah banyak penggunaan operasional.

Kelemahan dalam perangkat lunak komersial tidak hanya menghambat kinerja tetapi juga menciptakan kerentanan keamanan yang terbuka jaringan untuk penyusup. Setiap perusahaan keamanan tahun mengidentifikasi ribuan kerentanan perangkat lunak dalam perangkat lunak internet dan PC. Misalnya, pada tahun 2009, Symantec mengidentifikasi 384 kerentanan browser: 169 di Firefox, 94 di Safari, 45 di Internet Explorer, 41 di Chrome, dan 25 di Opera. Beberapa kerentanan ini kritis (Symantec, 2010).

Membenarkan kelemahan perangkat lunak setelah mereka diidentifikasi, vendor perangkat lunak menciptakan potongan-potongan kecil dari patch perangkat lunak yang disebut untuk memperbaiki kekurangan tanpa mengganggu operasi yang tepat dari perangkat lunak. Contohnya adalah Microsoft Windows Vista Service Pack 2, yang dirilis pada bulan April 2009, yang mencakup beberapa peningkatan keamanan untuk melawan malware dan hacker. Terserah pengguna perangkat lunak untuk melacak kerentanan ini, tes, dan menerapkan semua patch. Proses ini disebut manajemen patch.

Karena infrastruktur TI perusahaan biasanya sarat dengan aplikasi beberapa bisnis,

instalasi sistem operasi, dan layanan sistem lainnya, menjaga patch pada semua perangkat dan jasa yang digunakan oleh perusahaan sering memakan waktu dan mahal. Malware sedang dibuat sangat cepat sehingga perusahaan memiliki sedikit waktu untuk menanggapi antara waktu kerentanan dan patch diumumkan dan waktu perangkat lunak berbahaya muncul untuk mengeksploitasi kerentanan.

Kebutuhan untuk merespon begitu cepat ke torrent dari kerentanan keamanan bahkan menciptakan cacat dalam perangkat lunak dimaksudkan untuk memerangi mereka, termasuk produk antivirus populer. Apa yang terjadi pada musim semi 2010 untuk McAfee, vendor terkemuka perangkat lunak antivirus komersial adalah contoh, seperti Yang dibahas dalam Sidang .

[**Bisnis VAlue OF SECURITY DAN Control**](#_bookmark5)

Banyak perusahaan enggan menghabiskan banyak uang untuk keamanan karena tidak terkait langsung dengan pendapatan penjualan. Namun, melindungi sistem informasi sangat penting untuk operasi bisnis yang layak untuk dilihat kedua.

 Perusahaan memiliki aset informasi yang sangat berharga untuk dilindungi. Sistem sering menyimpan informasi rahasia tentang pajak individu, aset keuangan, rekam medis, dan tinjauan kinerja pekerjaan. Mereka juga dapat memuat informasi tentang operasi perusahaan, termasuk rahasia dagang, rencana pengembangan produk baru, dan strategi pemasaran. Sistem pemerintahan dapat menyimpan informasi tentang sistem persenjataan, operasi intelijen, dan target militer. Aset informasi ini memiliki nilai yang luar biasa, dan akibatnya dapat merusak jika mereka hilang, hancur, atau ditempatkan di tangan yang salah. Satu studi memperkirakan bahwa ketika keamanan perusahaan besar dikompromikan, perusahaan kehilangan sekitar 2,1 persen dari nilai pasarnya dalam dua hari dari pelanggaran keamanan, yang diterjemahkan ke dalam kerugian rata-rata $ 1,65 miliar dalam nilai pasar saham per insiden (Cavusoglu, Mishra, dan Raghunathan, 2004) keamanan tidak memadai dan kontrol dapat mengakibatkan kewajiban hukum yang serius. Bisnis harus melindungi tidak hanya aset informasi mereka sendiri tetapi juga orang-orang dari pelanggan, karyawan, dan mitra bisnis. Kegagalan untuk melakukannya dapat membuka perusahaan untuk litigasi mahal untuk paparan data atau pencurian. Sebuah organisasi dapat dimintai tanggung jawab untuk risiko perlu dan merugikan dibuat jika organisasi gagal untuk mengambil tindakan protektif yang sepatutnya untuk mencegah hilangnya informasi rahasia, data yang corrup- tion, atau pelanggaran privasi. Misalnya, Wholesale Club BJ digugat oleh

Komisi Perdagangan Federal AS untuk memungkinkan hacker untuk mengakses sistem dan mencuri kartu kredit dan debit data untuk pembelian penipuan. Bank yang mengeluarkan kartu dengan data yang dicuri dicari $ 13 juta dari BJ untuk mengimbangi mereka untuk pengembalian pemegang kartu untuk pembelian penipuan. Sebuah kerangka keamanan suara dan kontrol yang melindungi aset informasi bisnis sehingga dapat menghasilkan return yang tinggi atas investasi. keamanan yang kuat dan kontrol juga meningkatkan produktivitas karyawan dan biaya operasional yang lebih rendah.

**PERSYARATAN HUKUM DAN PERATURAN UNTUK PENGELOLAAN REKAMAN ELEKTRONIK**

peraturan pemerintah AS baru-baru ini memaksa perusahaan untuk mengambil keamanan dan kontrol lebih serius oleh mandat perlindungan data dari penyalahgunaan, paparan, dan akses yang tidak sah. Perusahaan menghadapi kewajiban hukum baru untuk retensi dan penyimpanan catatan elektronik serta untuk perlindungan privasi.

Jika Anda bekerja di industri perawatan kesehatan, perusahaan Anda akan perlu untuk mematuhi Asuransi Kesehatan Portabilitas dan Akuntabilitas Act (HIPAA) 1996. HIPAA menguraikan aturan dan prosedur keamanan medis dan privasi untuk menyederhanakan administrasi penagihan perawatan kesehatan dan mengotomatisasi transfer data kesehatan antara penyedia layanan kesehatan, pembayar, dan rencana. Hal ini membutuhkan anggota industri perawatan kesehatan untuk mempertahankan informasi pasien selama enam tahun dan menjamin kerahasiaan catatan-catatan. Ini menentukan privasi, keamanan, dan standar transaksi elektronik untuk penyedia layanan kesehatan penanganan informasi pasien, memberikan hukuman untuk pelanggaran privasi medis, pengungkapan catatan pasien melalui e-mail, atau akses jaringan yang tidak sah.

Jika Anda bekerja di sebuah perusahaan yang menyediakan jasa keuangan, perusahaan Anda akan perlu untuk mematuhi Jasa Keuangan Modernisasi Act of 1999, lebih dikenal sebagai Gramm-Leach-Bliley setelah sponsor kongres. Tindakan ini membutuhkan lembaga keuangan untuk menjamin keamanan dan kerahasiaan data pelanggan. Data harus disimpan pada media yang aman, dan langkah-langkah keamanan khusus harus ditegakkan untuk melindungi data tersebut pada media penyimpanan dan selama pengiriman.

Jika Anda bekerja di sebuah perusahaan publik, perusahaan Anda akan perlu untuk mematuhi Reformasi Akuntansi Perusahaan Publik dan Investor Protection Act of 2002, yang lebih dikenal sebagai Undang-Undang Sarbanes-Oxley setelah para sponsor Senator Paul Sarbanes dari Maryland dan Perwakilan Michael Oxley dari Ohio. Undang-undang ini dirancang untuk melindungi investor setelah skandal keuangan di Enron, WorldCom, dan perusahaan publik lainnya. Ini membebankan tanggung jawab pada perusahaan dan manajemen mereka untuk menjaga bersemangat dan integritas informasi keuangan yang digunakan secara internal dan eksternal dirilis tuduhannya. Salah satu Trek Belajar untuk bab ini membahas Sarbanes-Oxley secara rinci.

Karena sistem informasi yang digunakan untuk menghasilkan, menyimpan, dan trans- port data tersebut, undang-undang mengharuskan perusahaan untuk mempertimbangkan keamanan sistem informasi dan kontrol lain yang diperlukan untuk memastikan integritas, kerahasiaan, dan akurasi data mereka. Setiap aplikasi sistem yang berhubungan dengan data laporan keuangan yang kritis membutuhkan kontrol untuk memastikan data yang akurat. Kontrol untuk mengamankan jaringan perusahaan, mencegah akses tidak sah ke sistem dan data, dan memastikan integritas data dan ketersediaan di saat terjadi bencana atau gangguan lain dari layanan sangat penting juga.

BUKTI ELEKTRONIK DAN Forensik Komputer

Keamanan, kontrol, dan manajemen catatan elektronik telah menjadi penting untuk menanggapi tindakan hukum. Banyak bukti hari ini untuk penipuan saham, penggelapan, pencurian rahasia dagang perusahaan, kejahatan komputer, dan banyak kasus perdata dalam bentuk digital. Selain informasi dari halaman yang dicetak atau ketikan, kasus hukum saat ini semakin bergantung pada bukti direpresentasikan sebagai data digital yang tersimpan pada disk portabel floppy, CD, dan komputer hard disk drive, serta dalam e-mail, pesan instan, dan e-commerce transaksi melalui Internet. E-mail saat ini jenis yang paling umum dari bukti elektronik.

Dalam tindakan hukum, perusahaan wajib menanggapi permintaan penemuan untuk akses ke informasi yang dapat digunakan sebagai bukti, dan perusahaan diwajibkan oleh hukum untuk menghasilkan data tersebut. Biaya menanggapi permintaan penemuan bisa sangat besar jika perusahaan memiliki kesulitan perakitan data yang dibutuhkan atau data yang telah rusak atau hancur. Pengadilan sekarang memberikan hukuman keuangan dan bahkan kriminal berat bagi kehancuran yang tidak tepat dari dokumen elektronik.

[**MENETAPKAN**](#_bookmark5) **KERANGKA UNTUK KEAMANAN DAN PENGENDALIAN**

Bahkan dengan alat keamanan terbaik, sistem informasi Anda tidak akan dapat diandalkan dan aman kecuali Anda tahu bagaimana dan di mana untuk menerapkannya. Anda harus tahu di mana perusahaan Anda berisiko dan kontrol apa yang harus Anda miliki untuk melindungi sistem informasi Anda. Anda juga perlu mengembangkan kebijakan keamanan dan rencana untuk menjaga bisnis Anda tetap berjalan jika sistem informasi Anda tidak beroperasi.

SISTEM INFORMASI KONTROL

Sistem informasi kontrol yang baik manual dan otomatis dan terdiri dari kedua kontrol umum dan pengendalian aplikasi. kontrol umum mengatur desain, keamanan, dan penggunaan program komputer dan keamanan file data secara umum seluruh infrastruktur teknologi informasi organisasi. Secara keseluruhan, kontrol umum berlaku untuk semua aplikasi komputerisasi dan terdiri dari kombinasi hardware, software, dan prosedur manual yang menciptakan lingkungan kontrol secara keseluruhan.

Kontrol umum termasuk kontrol perangkat lunak, kontrol perangkat keras fisik, kontrol operasi komputer, kontrol keamanan data, kontrol atas implemen- tasi dari proses sistem, dan kontrol administratif. Tabel 8-3 menjelaskan fungsi dari masing-masing kontrol ini.

**kontrol aplikasi** adalah kontrol tertentu unik untuk setiap komputerisasi

aplikasi, seperti gaji atau pemrosesan order. Mereka termasuk kedua prosedur otomatis dan manual yang memastikan bahwa data hanya berwenang yang lengkap dan akurat diproses oleh aplikasi tersebut. Kontrol aplikasi dapat diklasifikasikan sebagai (1) kontrol input, (2) kontrol pengolahan, dan (3) kontrol output. masukan kontrol memeriksa data untuk akurasi dan kelengkapan ketika mereka memasuki sistem. Ada masukan kontrol khusus untuk otorisasi input, konversi data, mengedit data, dan penanganan error. kontrol pengolahan menetapkan bahwa data yang lengkap dan akurat selama memperbarui. output kontrol memastikan bahwa

hasil pemrosesan komputer adalah akurat, lengkap, dan didistribusikan dengan baik. Anda dapat menemukan detail lebih lanjut tentang aplikasi dan kontrol umum di Trek Pembelajaran kami.

TUGAS BERESIKO

Sebelum perusahaan Anda berkomitmen sumber daya untuk kontrol keamanan dan sistem informasi, harus tahu mana aset membutuhkan perlindungan dan sejauh mana aset tersebut rentan. Sebuah penilaian risiko membantu menjawab pertanyaan-pertanyaan ini dan menentukan set biaya yang paling efektif kontrol untuk melindungi aset.

Sebuah penilaian risiko menentukan tingkat risiko kepada perusahaan jika activ- tertentu

ity atau proses tidak terkontrol dengan baik. Tidak semua risiko dapat diantisipasi dan diukur, tetapi sebagian besar bisnis akan dapat memperoleh beberapa pemahaman tentang risiko yang mereka hadapi. manajer bisnis bekerja dengan spesialis sistem informasi harus mencoba untuk menentukan nilai aset informasi, poin kerentanan, frekuensi kemungkinan masalah, dan potensi kerusakan. Sebagai contoh, jika sebuah peristiwa yang mungkin terjadi tidak lebih dari sekali setahun, dengan maksimum dari $ 1.000 kerugian kepada organisasi, itu tidak bijaksana untuk menghabiskan $ 20.000 pada desain dan pemeliharaan kontrol untuk melindungi terhadap peristiwa itu. Namun, jika acara yang sama bisa terjadi setidaknya sekali sehari, dengan potensi kerugian lebih dari $ 300.000 setahun, $ 100.000 dihabiskan untuk kontrol mungkin sepenuhnya tepat.

KEBIJAKAN KEAMANAN

Setelah Anda mengidentifikasi risiko utama untuk sistem Anda, perusahaan Anda perlu mengembangkan kebijakan keamanan untuk melindungi aset perusahaan. Kebijakan keamanan terdiri atas pernyataan yang memeringkat risiko informasi, mengidentifikasi sasaran keamanan yang dapat diterima, dan mengidentifikasi mekanisme untuk mencapai sasaran-sasaran ini. Apa aset informasi terpenting perusahaan? Siapa yang menghasilkan dan mengontrol informasi ini di perusahaan? Apa kebijakan keamanan yang ada untuk melindungi informasi? Berapa tingkat risiko yang bersedia diterima manajemen untuk masing-masing aset ini? Apakah itu mau, misalnya, kehilangan data kredit pelanggan setiap 10 tahun sekali? Atau apakah akan membangun sistem keamanan untuk data kartu kredit yang dapat menahan bencana sekali dalam seratus tahun? Manajemen harus memperkirakan berapa biaya untuk mencapai tingkat risiko yang dapat diterima ini.

Kebijakan keamanan mendorong kebijakan yang menentukan penggunaan sumber daya informasi perusahaan yang dapat diterima dan anggota perusahaan mana yang memiliki akses ke aset informasinya. Kebijakan penggunaan yang dapat diterima (AUP) mendefinisikan penggunaan yang dapat diterima dari sumber daya informasi perusahaan dan peralatan komputasi, termasuk komputer desktop dan laptop, perangkat nirkabel, telepon, dan Internet. Kebijakan tersebut harus menjelaskan kebijakan perusahaan mengenai privasi, tanggung jawab pengguna, dan penggunaan pribadi dari peralatan dan jaringan perusahaan. AUP yang baik mendefinisikan tindakan yang tidak berterima dan dapat diterima untuk setiap pengguna dan menetapkan konsekuensi untuk ketidakpatuhan. Misalnya, kebijakan keamanan di Unilever, perusahaan barang konsumen multinasional raksasa, mengharuskan setiap karyawan yang dilengkapi dengan laptop atau perangkat genggam seluler untuk menggunakan perangkat yang ditentukan perusahaan dan menggunakan kata sandi atau metode identifikasi lainnya saat masuk ke jaringan perusahaan . Kebijakan keamanan juga mencakup ketentuan untuk manajemen identitas. Manajemen identitas terdiri dari proses bisnis dan perangkat lunak untuk mengidentifikasi pengguna sistem yang valid dan mengendalikan akses mereka ke sumber daya sistem. Ini mencakup kebijakan untuk mengidentifikasi dan mengotorisasi berbagai kategori pengguna sistem, menentukan sistem atau bagian apa dari sistem yang dapat diakses setiap pengguna, serta proses dan teknologi untuk mengautentikasi pengguna dan melindungi identitas mereka.

PERENCANAAN PEMULIHAN BENCANA DAN KELANJUTAN PERENCANAAN BISNIS

Jika Anda menjalankan bisnis, Anda perlu merencanakan untuk acara, seperti listrik padam, banjir, gempa bumi, atau serangan teroris yang akan mencegah informasi tems sistematis dan bisnis Anda dari operasi. Pemulihan bencana devisa perencanaan berencana untuk pemulihan komputasi dan komunikasi jasa setelah mereka telah terganggu. rencana pemulihan bencana fokus terutama pada masalah teknis yang terlibat dalam menjaga sistem dan berjalan, seperti yang file cadangan dan pemeliharaan sistem komputer cadangan atau layanan pemulihan bencana.

Sebagai contoh, MasterCard mempertahankan pusat komputer duplikat di Kansas City, Missouri, untuk melayani sebagai cadangan darurat untuk pusat komputer utama di St Louis. Daripada membangun mereka fasilitas backup sendiri, banyak perusahaan kontrak dengan perusahaan pemulihan bencana, seperti Comdisco Disaster Recovery Jasa di Rosemont, Illinois, dan SunGard Ketersediaan Services, berkantor pusat di Wayne, Pennsylvania. perusahaan pemulihan bencana ini menyediakan hot lokasi perumahan komputer cadang di lokasi di seluruh negeri di mana berlangganan perusahaan dapat menjalankan aplikasi kritis mereka dalam keadaan darurat. Misalnya, Juara Technologies, yang memasok bahan kimia yang digunakan dalam operasi minyak dan gas, mampu beralih sistem enterprise dari Houston ke situs panas SunGard di Scottsdale, Arizona, dalam dua jam.

 **perencanaan kelangsungan bisnis** berfokus pada bagaimana perusahaan

dapat mengembalikan busi-ness operasi setelah bencana terjadi. Rencana kesinambungan bisnis mengidentifikasi proses bisnis penting dan menentukan rencana aksi untuk menangani fungsi mission-critical jika sistem turun. Sebagai contoh, Deutsche Bank, yang menyediakan layanan perbankan investasi dan manajemen aset di 74 negara yang berbeda, memiliki rencana kesinambungan bisnis yang berkembang dengan baik bahwa itu terus update dan memurnikan. Ia memelihara tim penuh waktu di Singapura, Hong Kong, Jepang, India, dan Australia untuk mengkoordinasikan rencana mengatasi hilangnyafasilitas, personil, atau sistem kritis sehingga perusahaan dapat terus beroperasi ketika peristiwa bencana terjadi. Rencana Deutsche Bank membedakan antara proses penting untuk kelangsungan hidup bisnis dan orang-orang penting untuk dukungan krisis dan dikoordinasikan dengan perencanaan pemulihan bencana perusahaan untuk pusat komputernya. Manajer bisnis dan spesialis teknologi informasi perlu bekerja sama pada kedua jenis rencana untuk menentukan sistem dan proses bisnis yang paling penting untuk perusahaan. Mereka harus melakukan analisis dampak bisnis untuk mengidentifikasi sistem yang paling penting perusahaan dan dampak pemadaman sistem akan memiliki pada bisnis. Manajemen harus menentukan jumlah maksimum waktu bisnis dapat bertahan hidup dengan sistem yang turun dan bagian mana dari bisnis harus dipulihkan pertama.

PERAN AUDIT

Bagaimana manajemen tahu bahwa keamanan sistem informasi dan kontrol yang efektif? Untuk menjawab pertanyaan ini, organisasi harus melakukan sive comprehen- dan audit yang sistematis. Audit MIS meneliti lingkungan keamanan secara keseluruhan perusahaan serta kontrol yang mengatur sistem informasi individu. auditor harus melacak aliran transaksi sampel melalui sistem dan melakukan tes, menggunakan, jika sesuai, perangkat lunak audit otomatis. MIS Audit juga dapat memeriksa kualitas data.

Keamanan tinjauan audit teknologi, prosedur, dokumentasi, pelatihan, dan personil. Sebuah audit menyeluruh bahkan akan mensimulasikan serangan atau bencana untuk menguji respon dari teknologi, staf sistem informasi, dan karyawan bisnis.

Daftar audit dan peringkat semua kelemahan kontrol dan memperkirakan ity probabil- terjadinya. Kemudian menilai dampak keuangan dan organisasi masing-masing ancaman. Gambar 8-4 adalah daftar sampel auditor dari kelemahan kontrol untuk sistem pinjaman. Ini termasuk bagian untuk memberitahukan pengelolaan nesses weak- tersebut dan tanggapan manajemen. Manajemen diharapkan untuk menyusun rencana untuk melawan kelemahan signifikan dalam kontrol.

[**TECHNOLOGIES DAN Tools UNTUK PROTECTING sayaNFORMASI Resources**](#_bookmark5)

Bisnis memiliki sebuah array dari teknologi untuk melindungi sumber informasi mereka. Mereka termasuk alat untuk mengelola identitas pengguna, mencegah akses thorized unau- ke sistem dan data, memastikan ketersediaan sistem, dan memastikan kualitas perangkat lunak.

MANAJEMEN IDENTITAS DAN OTENTIKASI

perusahaan besar dan menengah memiliki infrastruktur TI yang kompleks dan banyak sistem yang berbeda, masing-masing dengan mengatur sendiri pengguna. perangkat lunak manajemen identitas mengotomatisasi proses melacak semua pengguna tersebut dan hak istimewa sistem mereka, menetapkan setiap pengguna identitas digital yang unik untuk mengakses setiap sistem. Hal ini juga mencakup perangkat untuk otentikasi pengguna, melindungi identitas pengguna, dan mengontrol akses ke sumber daya sistem.Untuk mendapatkan akses ke sistem, pengguna harus resmi dan dikonfirmasi. Otentikasi sering didirikan dengan menggunakan password yang hanya diketahui pengguna yang berwenang. Pengguna akhir menggunakan password untuk login ke sistem komputer dan juga dapat menggunakan password untuk mengakses sistem dan file tertentu. Namun, pengguna sering lupa password, berbagi, atau memilih password miskin yang mudah ditebak, yang mengganggu keamanan. sistem sandi yang produktivitas menghalangi karyawan terlalu ketat. Ketika karyawan harus mengubah password yang kompleks sering, mereka sering mengambil jalan pintas, seperti memilih password yang mudah ditebak atau menuliskan password mereka di stasiun-kerja mereka terlihat jelas. Password juga bisa “mengendus” jika dikirimkan melalui sebuah karya net- atau dicuri melalui rekayasa sosial.

Teknologi otentikasi baru, seperti token, smart card, dan otentikasi ric biomet-, mengatasi beberapa masalah ini. Token adalah perangkat fisik, mirip dengan kartu identitas, yang dirancang untuk membuktikan identitas pengguna tunggal. Token adalah gadget kecil yang biasanya muat pada gantungan kunci dan layar passcode yang sering berubah. Kartu pintar adalah perangkat seukuran kartu kredit yang berisi chip diformat dengan izin akses dan data lainnya. (Smart card juga digunakan dalam sistem pembayaran elektronik.) Sebuah perangkat pembaca menafsirkan data pada kartu cerdas dan memungkinkan atau menolak akses.

**otentikasi biometrik**menggunakan sistem yang membaca dan menafsirkan sifat-sifat individu manusia, seperti sidik jari, iris, dan suara-suara, untuk memberikan atau menolak akses. otentikasi biometrik didasarkan pada pengukuran sifat fisik atau perilaku yang membuat setiap individu unik. Ini membandingkan karakteristik unik seseorang, seperti sidik jari, wajah, atau gambar retina, terhadap profil disimpan karakteristik ini untuk menentukan apakah ada menggambarkan perbedaan antara karakteristik ini dan profil disimpan. Jika dua profil sesuai, akses diberikan. Sidik jari dan teknologi pengenalan wajah baru mulai digunakan untuk aplikasi keamanan, dengan banyak laptop PC yang dilengkapi dengan perangkat identifikasi sidik jari dan beberapa model dengan built-in webcam dan perangkat lunak pengenalan wajah.

**Firewall, Intrusion Detection Systems, & Software Anti virus**

Tanpa perlindungan terhadap malware dan penyusup, menghubungkan ke Internet akan sangat berbahaya. Firewall, sistem deteksi intrusi, dan perangkat lunak antivirus telah menjadi alat bisnis yang penting.

**firewall**

**firewall** mencegah pengguna yang tidak sah mengakses jaringan pribadi. Firewall adalah kombinasi dari hardware dan software yang mengontrol arus lalu lintas jaringan yang masuk dan keluar. Hal ini umumnya ditempatkan antara jaringan internal yang swasta organisasi dan jaringan eksternal tidak mempercayai, seperti Internet, meskipun firewall juga dapat digunakan untuk melindungi satu bagian dari jaringan haan com- dari sisa jaringan. Firewall bertindak seperti gatekeeper yang meneliti mandat masing-masing pengguna sebelum akses diberikan ke jaringan. Firewall mengidentifikasi nama, alamat IP, aplikasi, dan karakteristik lain dari lalu lintas masuk. Ia memeriksa informasi ini terhadap aturan akses yang telah diprogram ke dalam sistem oleh administrator jaringan. Firewall mencegah munication com- tidak sah ke dalam dan keluar dari jaringan.

*Paket penyaringan*

Memeriksa bidang yang dipilih dalam header dari paket data yang mengalir bolak-balik antara jaringan terpercaya dan Internet, memeriksa paket vidual puncak-dalam isolasi. Teknologi penyaringan ini dapat kehilangan banyak jenis serangan. inspeksi stateful menyediakan keamanan tambahan dengan menentukan apakah paket adalah bagian dari dialog-dialog antara pengirim dan penerima. Ini set up meja negara untuk melacak informasi lebih beberapa paket. Paket diterima atau ditolak berdasarkan apakah mereka adalah bagian dari percakapan disetujui atau apakah mereka mencoba untuk membuat sambungan yang sah.

*Network Address Translation (NAT)* dapat memberikan lapisan perlindungan

ketika penyaringan paket statis dan inspeksi stateful bekerja. NAT menyembunyikan alamat IP komputer host internal organisasi (s) untuk mencegah program sniffer luar firewall dari memastikan mereka dan menggunakan informasi tersebut untuk menembus sistem internal.

*Aplikasi proxy filtering* memeriksa isi aplikasi paket.

Sebuah server proxy berhenti paket data yang berasal di luar organisasi, memeriksa mereka, dan melewati proxy ke sisi lain dari firewall. Jika pengguna di luar perusahaan ingin berkomunikasi dengan pengguna dalam organisasi, luar pengguna pertama “pembicaraan” dengan aplikasi proxy dan aplikasi proxy berkomunikasi dengan komputer internal perusahaan. Demikian juga, pengguna komputer dalam organisasi melewati proxy untuk berbicara dengan komputer di luar.

**Sistem Deteksi intrusi**

Selain firewall, vendor keamanan komersial sekarang menyediakan alat-alat dan layanan deteksi intrusi untuk melindungi terhadap lalu lintas jaringan yang mencurigakan dan upaya untuk mengakses file dan database. sistem deteksi intrusi fitur alat pemantauan penuh waktu ditempatkan pada titik-titik paling rentan atau “hot spot” dari jaringan perusahaan untuk mendeteksi dan mencegah penyusup terus. Sistem gen- erates alarm jika menemukan peristiwa yang mencurigakan atau anomali. perangkat lunak pemindaian mencari pola menunjukkan metode yang dikenal serangan komputer, seperti password yang buruk, memeriksa untuk melihat apakah file penting telah dihapus atau diubah, dan mengirimkan peringatan vandalisme atau sistem administrasi kesalahan. Pemantauan perangkat lunak meneliti peristiwa seperti yang terjadi untuk menemukan serangan keamanan berlangsung.

**Antivirus dan Antispyware Software**

rencana teknologi defensif untuk kedua individu dan bisnis harus mencakup perlindungan antivirus untuk setiap komputer. Perangkat lunak antivirus dirancang untuk memeriksa sistem komputer dan drive untuk kehadiran virus komputer. Seringkali perangkat lunak menghilangkan virus dari daerah yang terinfeksi. Namun, sebagian besar perangkat lunak antivirus hanya efektif terhadap virus yang sudah dikenal ketika perangkat lunak ditulis. Untuk tetap efektif, perangkat lunak antivirus harus con tinually diperbarui. produk antivirus yang tersedia untuk berbagai jenis perangkat mobile dan handheld selain server, workstation, dan PC desktop.

vendor software antivirus terkemuka, seperti McAfee, Symantec, dan Trend Micro, telah meningkatkan produk mereka untuk memasukkan perlindungan terhadap spyware. perangkat lunak antispyware seperti Ad-Aware, Spybot S & D, dan Spyware Doctor juga sangat membantu.

**Sistem Manajemen Unified Threat**

Untukmembantu bisnis mengurangi biaya dan meningkatkan pengelolaan, vendor keamanan telah digabungkan menjadi satu alat berbagai alat keamanan, termasuk dinding dengan kebakaran hutan, jaringan pribadi virtual, sistem deteksi intrusi, dan penyaringan konten Web dan perangkat lunak antispam. Produk-produk manajemen keamanan yang komprehensif disebut unified threat management (UTM) sistem. Meskipun pada awalnya ditujukan untuk businesss kecil dan menengah, produk UTM yang avail- mampu untuk semua ukuran jaringan. vendor UTM terkemuka termasuk palang, Fortinent, dan Check Point, dan jaringan vendor seperti Cisco Systems dan Juniper Networks menyediakan beberapa kemampuan UTM dalam peralatan mereka.

Mengamankan JARINGAN WIRELESS

Meskipun kekurangan, WEP menyediakan beberapa margin keamanan jika pengguna Wi-Fi mengingat kode untuk mengaktifkannya. Langkah pertama yang sederhana untuk menggagalkan hacker adalah untuk menetapkan nama unik untuk jaringan Anda SSID dan menginstruksikan router Anda untuk tidak menyiarkannya. Perusahaan dapat lebih meningkatkan keamanan Wi-Fi dengan menggunakannya dalam hubungannya dengan teknologi virtual private network (VPN) ketika mengakses data internal perusahaan.

Pada bulan Juni 2004, kelompok industri perdagangan Wi-Fi Alliance diselesaikan spesifikasi 802.11i (juga disebut sebagai Wi-Fi Protected Access 2 atau WPA2) yang menggantikan WEP dengan standar keamanan yang lebih kuat. Alih-alih kunci enkripsi statis digunakan dalam WEP, standar baru

Sistem dengan server otentikasi pusat untuk memastikan bahwa pengguna hanya berwenang mengakses jaringan.

ENKRIPSI DAN PUBLIC KEY INFRASTRUKTUR

Banyak bisnis menggunakan enkripsi untuk melindungi informasi digital yang mereka simpan, mentransfer secara fisik, atau mengirim melalui Internet. Enkripsi adalah proses transformasi teks biasa atau data ke dalam teks cipher yang tidak dapat dibaca oleh orang lain selain pengirim dan penerima yang dituju. Data dienkripsi dengan menggunakan kode numerik rahasia, disebut kunci enkripsi, yang mengubah data biasa ke dalam teks cipher. pesan harus didekripsi oleh penerima.

Dua metode untuk mengenkripsi lalu lintas jaringan di Web adalah SSL dan S-HTTP. Secure Sockets Layer (SSL) dan penggantinya Transport Layer Security-nya (TLS) memungkinkan klien dan server komputer untuk mengelola kegiatan enkripsi dan dekripsi karena mereka berkomunikasi satu sama lain selama sesi Web aman. Aman Hypertext Transfer Protocol (S-HTTP) adalah protokol lain yang digunakan untuk mengenkripsi data yang mengalir melalui Internet, tetapi terbatas untuk pesan individu, sedangkan SSL dan TLS dirancang untuk membuat sambungan aman antara dua komputer.

Kemampuan untuk menghasilkan sesi aman dibangun ke klien Internet perangkat lunak browser dan server. Klien dan server menegosiasikan apa kunci dan apa tingkat keamanan untuk digunakan. Setelah sesi aman didirikan antara klien dan server, semua pesan di sesi yang dienkripsi.

Ada dua metode alternatif enkripsi: enkripsi kunci simetris dan enkripsi kunci publik. Dalam enkripsi kunci simetris, pengirim dan penerima membuat sesi Internet yang aman dengan membuat kunci enkripsi tunggal dan mengirimkannya ke penerima sehingga kedua pengirim dan penerima berbagi kunci yang sama. Kekuatan kunci enkripsi diukur dengan panjang bit-nya. Hari ini, kunci khas akan 128 bit panjang (string dari 128 digit biner).

Masalah dengan semua skema enkripsi simetris adalah bahwa kunci itu sendiri harus dibagi entah bagaimana antara pengirim dan penerima, yang memaparkan kunci untuk luar yang mungkin saja mampu mencegat dan mendekripsi kunci. Bentuk yang lebih aman dari enkripsi disebut enkripsi kunci publik menggunakan dua kunci: satu bersama (atau publik) dan satu benar-benar pribadi seperti yang ditunjukkan pada Gambar 8-6. Tombol yang matematis terkait sehingga data dienkripsi dengan satu kunci dapat didekripsi hanya menggunakan tombol lain. Untuk mengirim dan menerima pesan, Communication.

**sertifikat digital** adalah file data yang digunakan untuk menentukan identitas pengguna dataset elektronik untuk perlindungan dari transaksi online. Sebuah sistem sertifikat digital menggunakan pihak ketiga yang dipercaya, yang dikenal sebagai otoritas sertifikat (CA, atau otoritas sertifikasi), untuk memvalidasi identitas pengguna. Ada banyak CA di Amerika Serikat dan di seluruh dunia, termasuk VeriSign, IdenTrust, dan Australia KeyPost. CA memverifikasi identitas sertifikat pengguna digital offline. Informasi ini dimasukkan ke dalam server CA, yang menghasilkan informasi digital terenkripsi sertifikat yang berisi identifikasi pemilik dan salinan pemilik kunci publik. sertifikat akan mengotentikasi bahwa kunci publik milik pemilik yang ditunjuk desig-. CA membuat kunci publik sendiri tersedia untuk umum baik di media cetak atau mungkin di Internet. Penerima pesan terenkripsi menggunakan kunci publik CA untuk memecahkan kode sertifikat digital yang melekat pada pesan, memverifikasi itu dikeluarkan oleh CA, dan kemudian memperoleh kunci dan identifikasi informasi publik pengirim yang terkandung dalam sertifikat. Dengan menggunakan informasi ini, penerima dapat mengirim balasan terenkripsi. Sistem sertifikat digital akan memungkinkan, misalnya, pengguna kartu kredit dan pedagang untuk memvalidasi bahwa sertifikat digital mereka dikeluarkan oleh yang berwenang dan dipercaya pihak ketiga sebelum mereka bertukar data. infrastruktur kunci publik (PKI), penggunaan pub-kriptografi kunci lic bekerja dengan CA, kini banyak digunakan dalam e-commerce.

MEMASTIKAN SYSTEM KETERSEDIAAN

Sebagai perusahaan semakin bergantung pada jaringan digital untuk pendapatan dan operasi, mereka perlu mengambil langkah-langkah tambahan untuk memastikan bahwa sistem dan aplikasi mereka

selalu tersedia. Perusahaan seperti di industri penerbangan dan jasa keuangan dengan aplikasi kritis yang membutuhkan pemrosesan transaksi online secara tradisional digunakan sistem komputer toleransi kegagalan selama bertahun-tahun untuk memastikan ketersediaan 100 persen. Dalam proses transaksi online, tions transac- masuk secara online segera diproses oleh komputer. Perubahan beraneka ragam untuk database, pelaporan, dan permintaan untuk informasi terjadi setiap instan.

**sistem komputer toleran** mengandung berlebihan hardware, software,

dan power supply komponen yang menciptakan lingkungan yang menyediakan terus menerus, tanpa gangguan layanan. komputer toleran menggunakan rutin gudang soft khusus atau logika diri memeriksa dibangun ke sirkuit mereka untuk mendeteksi kegagalan hardware dan secara otomatis beralih ke perangkat cadangan. Bagian dari ini ers comput- dapat dihapus dan diperbaiki tanpa gangguan terhadap sistem komputer.

Toleransi kesalahan harus dibedakan dari komputasi ketersediaan tinggi.

Kedua toleransi kesalahan dan komputasi ketersediaan tinggi mencoba untuk meminimalkan downtime. Downtime mengacu pada periode waktu di mana suatu sistem tidak operasional. Namun, komputasi ketersediaan tinggi membantu perusahaan segera pulih dari sistem crash, sedangkan toleransi kesalahan menjanjikan ketersediaan berkelanjutan dan penghapusan waktu pemulihan sama sekali.

**Pengendalian Lalu Lintas Jaringan: Deep Packet Inspection**Apakah Anda pernah mencoba untuk menggunakan jaringan kampus dan menemukan itu sangat lambat? Mungkin karena sesama siswa menggunakan jaringan untuk men-download musik atau menonton YouTube. aplikasi bandwidth memakan seperti program file-sharing, layanan telepon Internet, dan video online dapat menyumbat dan memperlambat jaringan perusahaan, menurunkan kinerja. Misalnya, bola Sate University di Muncie, Indiana, menemukan jaringan telah melambat karena minoritas kecil dari siswa menggunakan program file-sharing peer-to-peer untuk men-download film dan musik.

ISU KEAMANAN UNTUK CLOUD COMPUTING DAN MOBILE DIGITAL PLATFORM

Meskipun komputasi awan dan muncul Platform mobile digital memiliki potensi untuk memberikan manfaat yang kuat, mereka menimbulkan tantangan baru untuk keamanan dan keandalan sistem. Kami sekarang menggambarkan beberapa tantangan ini dan bagaimana mereka harus ditangani.

**Keamanan di Cloud**

Ketika pengolahan berlangsung di awan, akuntabilitas dan tanggung jawab untuk perlindungan data sensitif masih berada dengan perusahaan yang memiliki data tersebut. Memahami bagaimana penyedia komputasi awan mengatur layanan dan mengelola data yang penting. Sesi Interaktif Teknologi rincian beberapa masalah keamanan cloud yang harus ditangani.

**Mengamankan Platform Mobile**

Jika perangkat mobile yang melakukan banyak fungsi komputer, mereka harus dijamin seperti desktop dan laptop terhadap malware, pencurian, kerugian kecelakaan, akses yang tidak sah, dan upaya hacking. perangkat mobile mengakses sistem dan data perusahaan membutuhkan perlindungan khusus.

Perusahaan harus memastikan bahwa kebijakan keamanan perusahaan mereka termasuk perangkat mobile, dengan rincian tambahan tentang bagaimana perangkat mobile harus dukungan- porting, dilindungi, dan digunakan. Mereka akan membutuhkan alat untuk mengotorisasi semua perangkat yang digunakan; untuk mempertahankan catatan persediaan yang akurat pada semua perangkat mobile, pengguna, dan aplikasi; untuk mengontrol update ke aplikasi; dan untuk mengunci perangkat yang hilang sehingga mereka tidak dapat dikompromikan.

MEMASTIKAN KUALITAS SOFTWARE

Selain menerapkan keamanan dan kontrol yang efektif, organisasi dapat meningkatkan kualitas dan keandalan sistem dengan menggunakan metrik perangkat lunak dan pengujian perangkat lunak yang ketat. metrik perangkat lunak adalah penilaian obyektif dari sistem dalam bentuk pengukuran kuantitatif. penggunaan berkelanjutan metrik memungkinkan