MELINDUNGI SISTEM INFORMASI

Sistem Informasi Akuntansi

ELVIA PUSPA DEWI, S.KOM, M.AK

MELINDUNGI SISTEM INFORMASI

A. KERENTANAN DAN PENYALAHGUNAAN SISTEM

Jika terlalu banyak data hancur atau mengungkapkan, bisnis Anda mungkin tidak pernah dapat beroperasi! Singkatnya, jika Anda menjalankan bisnis hari ini, Anda perlu membuat keamanan dan mengendalikan prioritas utama. Keamanan tersebut dengan kebijakan, prosedur, dan teknis langkah-langkah yang digunakan untuk mencegah akses yang tidak sah, perubahan, pencurian, atau kerusakan fisik sistem informasi.

Kita tahu sistem informasi perlu dilindungi dari perusakan, kesalahan dan penyalahgunaan. Sebelumnya kita mengerti arti dari sistem informasi itu apa. Sistem informasi (information system) merupakan komponen yang saling terkait yang berkerja sama untuk mengumpulkan, memproses, menyimpan, dan menyebarkan informasi untuk mendukung pengambilan keputusan, koordinasi, pengendalian, analisis, dan visualisasi dalam organisasi.

1. Mengapa Sistem Menjadi Rentan

Gambar diatas menggambarkan ancaman yang paling umum terhadap sistem informasi kontemporer. Mereka bisa berasal dari teknis, organisasi, dan lingkungan faktor diperparah dengan keputusan manajemen yang buruk. Dalam multi-tier client / server lingkungan komputasi yang digambarkan di sini, kerentanan ada di setiap lapisan dan dalam komunikasi antara lapisan. Pengguna di klien lapisan dapat menyebabkan kerusakan dengan memperkenalkan kesalahan atau dengan mengakses sistem tanpa otorisasi. Hal ini dimungkinkan untuk mengakses data yang mengalir melalui jaringan, mencuri berharga data selama transmisi, atau mengubah pesan tanpa otorisasi. Radiasi dapat mengganggu jaringan di berbagai titik juga. Penyusup dapat memulai serangan denial-ofservice atau perangkat lunak berbahaya untuk mengganggu pengoperasian situs web.

Mereka mampu menembus sistem perusahaan dapat merusak atau mengubah perusahaan data yang disimpan dalam database atau file. Kesalahan dalam pemrograman, instalasi yang tidak tepat, atau perubahan tidak sah menyebabkan perangkat lunak komputer gagal. Gangguan listrik,

banjir, kebakaran, atau bencana alam lainnya dapat juga mengganggu sistem komputer. Kemitraan domestik atau luar negeri dengan perusahaan lain menambah sistem kerentanan jika informasi yang berharga berada pada jaringan dan komputer di luar pengendalian organisasi. Tanpa perlindungan yang kuat, data berharga bisa hilang, hancur, atau bisa jatuh ke tangan yang salah, mengungkapkan perdagangan penting rahasia atau informasi yang melanggar privasi pribadi.

Kerentanan Internet

Jaringan publik yang besar, seperti Internet, lebih rentan daripada internal yang jaringan karena mereka hampir terbuka bagi siapa saja. Internet adalah begitu besar bahwa ketika pelanggaran terjadi, mereka dapat memiliki dampak yang sangat besar luas. Ketika internet menjadi bagian dari jaringan perusahaan, organisasi sistem informasi 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.

Kerentanan juga meningkat dari meluasnya penggunaan e-mail, instant messaging (IM), dan program peer-to-peer file-sharing. E-mail dapat berisi lampiran yang berfungsi sebagai springboards untuk perangkat lunak berbahaya atau tidak sah akses ke sistem internal perusahaan.

Tantangan Keamanan Nirkabel

Jaringan nirkabel di Anda rumah rentan karena pita frekuensi radio yang mudah untuk memindai. Kedua Jaringan Bluetooth dan Wi-Fi yang rentan terhadap hacking dengan penyadap. Meskipun berbagai jaringan Wi-Fi hanya beberapa ratus kaki, itu bisa diperpanjang sampai dengan seperempat mil menggunakan antena eksternal.

Standar keamanan awal dikembangkan untuk Wi-Fi, disebut Wired Equivalent Privasi (WEP), sangat tidak efektif. WEP dibangun ke semua standar 802.11 produk, namun penggunaannya adalah opsional. Banyak pengguna mengabaikan untuk menggunakan fitur keamanan WEP, meninggalkan mereka terlindungi. Spesifikasi WEP dasar panggilan untuk jalur akses dan semua penggunanya untuk berbagi sama 40-bit password terenkripsi, yang dapat mudah didekripsi oleh hacker dari sejumlah kecil lalu lintas.

2. Peranti Lunak Berbahaya: Virus, Worm, Trojan Horse, Dan Spyware Hacker

Malware adalah program perantik lunak yang sangat berbahaya meliputi berbagai jenis ancaman seperti *virus komputer*, *worm*, *trojan horses*, dan *spyware*. Komputer virusi program perangkat lunak jahat yang menempel pada perangkat lunak lain program atau file data untuk dieksekusi, biasanya tanpa pengetahuan pengguna atau izin. Virus biasanya menyebar dari komputer ke komputer ketika manusia mengambil tindakan, seperti mengirim lampiran e-mail atau menyalin file yang terinfeksi. Untuk itu kita terlebih dahulu dapat mengetahui arti ataupun pengertian dari virus-virus yang berbahaya dalam perantik lunak tersebut antara lain sebagai berikut.

- Virus komputer adalah program aplikasi yang bertujuan untuk dijalankan yang terhubung dengan sendirinya dengan program aplikasi perantik lunak lainya atau data, sering menyebabkan perantik keras dan lunak tidak berfungsi dengan baik. Dengan kata lain program perantik lunak berbahaya yang menempelkan dirinya ke program lainnya atau file data untuk dieksekusi, biasanya tanpa sepengetahuan atau seizing pengguna.
- Worm adalah program perantik lunak yang menyebar dengan sendirinya untuk mengganggu operasional jaringan komputer atau menghancurkan data dan program lainnya.
- Trojan Horses adalah program perantik lunak yang tampaknya tidak berbahaya tapi justru berbuat sesuatu yang tidak diperkirakan.
- Spyware adalah teknologi yang membantu mengumpulkan informasi tentang seseorang atau organisasi tanpa sepengetahuan mereka. Program kecil ini memasang diri secara sembunyi-sembunyi di komputer untuk memantau kegiatan penelusuran web oleh pengguna komputer dan untuk memunculkan iklan.

Virus Komputer dan *Worm* dapat merajalela dari satu sistem ke sistem lain, memakan memori computer atau menghancurkan program dan data komputer. Worm dan virus yang sering menyebar melalui Internet dari file software download, dari file yang melekat pada transmisi e-mail, atau dari pesan e-mail dikompromikan atau pesan instan. Begitu pun *Trojan Horses* dan *Spyware*, secara tidak diperkirakan dapat berbahaya bagi peranti lunak dan dapat mengganggu dalam membuka sebuah web.

3. Hacker Dan Kejahatan Komputer

Seorang hacker adalah seorang individu yang bermaksud untuk mendapatkan akses tidak sah ke dalam sistem komputer. Dalam komunitas hacker, istilah cracker biasanya digunakan untuk

menunjukkan bahwa seorang hacker adalah kriminal. Hacker dan cracker memperoleh akses yang sah dengan mencari kelemahan dalam perlindungan keamanan yang dipekerjakan oleh Situs web dan sistem komputer. Seiring dengan seringnya seorang hacker mengambil keuntungan dari berbagai fitur dalam internet, maka sistem pun jauh lebih terbuka dan membuatnya jauh lebih mudah untuk digunakan. Kegiatan hacker telah diperluas di luar intrusi sistem dengan memasukkan pencurian identitas dan informasi, kerusakan sistem dan *Click Fraud*, atau bahkan *Cyberterrorism* dan *Cyberwarfare*.

- **Pencurian Identitas** adalah : Pencurian bagian kuncul dari informasi pribadi atau kejahatan di mana seorang penipu mendapatkan informasi yang penting, seperti kartu kredit atau nomor jaminan sosial dengan tujuan mendapatkan layanan atas nama korban atau untuk mendapatkan data rahasia yang tidak tepat. Pencurian identitas telah berkembang pesat di internet. File kartu kredit adalah sasaran utama para hacker situs web. Situs e-commerce adalah sumber informasi pribadi yang luar biasa karena menyimpan nama, alamat, dan nomor telepon.

Phising adalah bentuk penipuan melibatkan pembuatan halaman situs palsu atau pesan elektronik (e-mail) seolah-olah berasal dari pihak yang sah dan menanyakan data pribadi yang rahasia.

Pharming adalah Teknik phising yang mengarahkan pengguna ke halaman situs web palsu, bahkan saat seseorang mengetikkan alamat halaman situs yang seharusnya.

- **Click Fraud (penipuan lewat klik)** adalah : mengklik dengan curang iklan online berbayar untuk mengahasilkan biaya per klik yang tak semestinya. Penipuan lewat klik terjadi seseorang atau program computer dengan curang mengeklik sebuah iklan online tanpa maksud mempelajari lebih lanjut tentang pemasangan iklannya atau melakukan pembelian.

- ***Cyberterrorism*** dan ***Cyberwarfare***. , semakin besar perhatian difokuskan pada kerentanan internet atau jaringan lainnya yang dapat dimanfaatkan oleh teroris, badan intel luar negeri atau kelompok lain untuk menciptakan gangguan dan bahaya luas. Serangan maya seperti itu sasaranya mungkin berupa perantik lunak yang menjalankan pembagian listrik, mengendalikan lalu lintas udara atau jaringan bank-bank atau institusi keuangan besar.

4. Ancaman Internal: Karyawan

Kita cenderung berfikir bahwa ancaman keamanan untuk bisnis berasal dari luar organisasi. Bahkan, orang dalam perusahaan menimbulkan masalah keamanan serius. Contohnya saja karyawan, karyawan bisa saja memiliki akses pada informasi rahasia, dan dengan adanya kecerobohan pada intern sistem prosedur keamanan, mereka bisa saja mampu untuk menjelajah ke

seluruh organisasi sistem tanpa meninggalkan jejak. Studi telah menemukan bahwa kurangnya pengetahuan dari pengguna adalah penyebab tunggal terbesar dari pelanggaran keamanan jaringan. Banyak karyawan lupa password mereka untuk mengakses sistem komputer atau mengizinkan rekan kerja untuk menggunakannya, yang mengabaikan sistem. kadang-kadang penyusup berbahaya mencari akses sistem karyawan mengungkapkan password mereka dengan berpura-pura menjadi anggota yang sah dari perusahaan. Praktek ini disebut social engineering. Pengguna dan sistem informasi baik akhir spesialis juga merupakan sumber utama kesalahan yang diperkenalkan ke dalam sistem informasi.

5. Kerentanan Peranti Lunak (Software)

Kesalahan perangkat lunak menimbulkan ancaman konstan untuk sistem informasi, menyebabkan tak terhitung kerugian dalam produktivitas. Tumbuh kompleksitas dan ukuran program perangkat lunak, ditambah dengan tuntutan untuk pengiriman tepat waktu ke pasar, telah memberikan kontribusi untuk peningkatan kelemahan perangkat lunak atau kerentanan. Masalah utama dengan perangkat lunak adalah adanya bug atau program tersembunyi cacat kode. Penelitian telah menunjukkan bahwa hampir tidak mungkin untuk menghilangkan semua bug dari program besar. Sumber utama bug adalah kompleksitas keputusan membuat kode. Sebuah program yang relatif kecil dari beberapa ratus baris akan berisi puluhan keputusan yang mengarah ke ratusan atau bahkan ribuan jalan yang berbeda.

B. NILAI BISNIS DARI PENGAMANAN DAN PENGENDALIAN

Banyak perusahaan enggan untuk menghabiskan berat pada keamanan karena tidak langsung terkait dengan pendapatan penjualan. Namun, melindungi sistem informasi begitu penting untuk operasi bisnis yang layak melihat kedua. Perusahaan memiliki aset informasi yang sangat berharga untuk melindungi. Sistem sering rumah informasi rahasia tentang individu 'pajak, aset keuangan, catatan medis, dan ulasan kinerja pekerjaan. Mereka juga dapat berisi informasi pada operasi perusahaan, termasuk rahasia dagang, pengembangan produk baru rencana, dan strategi pemasaran. Sistem pemerintah dapat menyimpan informasi pada sistem senjata, operasi intelijen, dan sasaran militer. Informasi ini aset memiliki nilai yang sangat besar, dan akibatnya dapat menghancurkan jika mereka hilang, rusak, atau ditempatkan di tangan yang salah.

Keamanan dan kontrol yang tidak memadai dapat menyebabkan tanggung jawab hukum serius. Bisnis harus melindungi tidak hanya aset informasi mereka sendiri tetapi juga orang-orang

dari pelanggan, karyawan, dan mitra bisnis. Kegagalan untuk melakukan hal ini dapat membuka tegas untuk litigasi mahal untuk pemaparan data atau pencurian. Sebuah organisasi dapat diadakan bertanggung jawab atas risiko perlu dan merugikan dibuat jika organisasi gagal untuk mengambil tepat tindakan protektif untuk mencegah hilangnya informasi rahasia, data korupsi, atau pelanggaran privasi.

1. Persyaratan Hukum Dan Peraturan Untuk Manajemen Catatan Elektronik

Peraturan pemerintah AS baru-baru ini memaksa perusahaan untuk mengambil keamanan dan mengendalikan lebih serius oleh mandat perlindungan data dari penyalahgunaan, eksposur, dan akses yang tidak sah. Perusahaan menghadapi kewajiban hukum baru untuk retensi dan penyimpanan catatan elektronik serta untuk perlindungan privasi. Data harus disimpan pada media yang aman, dan keamanan khusus tindakan harus ditegakkan untuk melindungi data tersebut pada media penyimpanan dan selama pengiriman.

Sarbanes-Oxley pada dasarnya adalah tentang memastikan bahwa kontrol internal di tempat untuk mengatur penciptaan dan dokumentasi informasi dalam laporan keuangan. Karena sistem informasi yang digunakan untuk menghasilkan, menyimpan, dan transportasi. Data tersebut, undang-undang mengharuskan perusahaan untuk memper timbangkan sistem informasi keamanan dan kontrol lain yang diperlukan untuk menjamin integritas, kerahasiaan, dan akurasi data mereka.

2. Bukti Elektronik Dan Ilmuforensik Komputer

Forensicsis computer koleksi ilmiah, pemeriksaan, otentikasi, pelestarian, dan analisis data diadakan pada atau diambil dari media penyimpanan komputer sedemikian rupa bahwa informasi dapat digunakan sebagai bukti dalam pengadilan. Ini berkaitan dengan berikut ini masalah:

- Memulihkan data dari komputer sambil menjaga integritas bukti
- Aman menyimpan dan penanganan data elektronik pulih
- Mencari informasi yang signifikan dalam volume besar data elektronik
- Menyajikan informasi untuk pengadilan

Bukti elektronik mungkin berada pada media penyimpanan komputer dalam bentuk file komputer dan data sebagai ambient, yang tidak terlihat oleh pengguna rata-rata. Sebuah contoh mungkin file yang telah dihapus pada PC hard drive. Data bahwa pengguna komputer mungkin telah dihapus pada media penyimpanan komputer dapat dipulihkan melalui berbagai teknik. Ahli

forensik komputer mencoba untuk memulihkan seperti Data tersembunyi untuk presentasi sebagai bukti. Kesadaran forensik komputer harus dimasukkan ke dalam suatu perusahaan proses perencanaan kontingensi.

C. MENETAPKAN KERANGKA KERJA UNTUK PENGAMANAN DAN PENGENDALIAN

Bahkan dengan alat-alat keamanan terbaik, sistem informasi Anda tidak akan dapat diandalkan dan aman kecuali jika Anda tahu bagaimana dan di mana untuk menempatkan mereka. Anda harus tahu di mana perusahaan Anda berisiko dan apa kontrol Anda harus memiliki di tempat untuk melindungi sistem informasi Anda. Anda juga akan perlu mengembangkan keamanan rencana kebijakan dan untuk menjaga bisnis Anda berjalan jika sistem informasi Anda tidak operasional.

1. Sistem Informasi Kontrol

Kontrol sistem informasi yang baik manual dan otomatis dan terdiri dari kedua kontrol umum dan pengendalian aplikasi. Secara keseluruhan, kontrol umum berlaku untuk semua aplikasi komputerisasi dan terdiri dari kombinasi prosedur hardware, software, dan manual yang menciptakan lingkungan kontrol secara keseluruhan. Kontrol umum mencakup kontrol perangkat lunak, perangkat keras kontrol fisik, kontrol operasi komputer, kontrol keamanan data, kontrol atas pelaksanaan proses sistem, dan kontrol administratif. Kontrol aplikasi dapat diklasifikasikan sebagai (1) kontrol input, (2) kontrol pengolahan, dan (3) kontrol output. Kontrol input memeriksa data untuk akurasi dan kelengkapan ketika mereka memasuki sistem. Ada kontrol input khusus untuk otorisasi input, data yang konversi, editing data, dan penanganan error. Kontrol pengolahan menetapkan bahwa Data yang lengkap dan akurat selama memperbarui. Output kontrol memastikan bahwa hasil pemrosesan komputer yang akurat, lengkap, dan benar didistribusikan.

2. Penilaian Risiko

Sebelum perusahaan Anda berkomitmen sumber daya untuk keamanan dan sistem informasi kontrol, ia harus tahu aset yang 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 ke perusahaan jika aktivitas spesifik atau proses tidak terkontrol dengan baik. Tidak semua risiko bisa diantisipasi dan diukur, tetapi

sebagian besar bisnis akan dapat memperoleh beberapa pemahaman tentang risiko yang mereka hadapi. Manajer bisnis bekerja dengan sistem informasi spesialis harus mencoba untuk menentukan nilai aset informasi, poin dari kerentanan, frekuensi kemungkinan masalah, dan potensi kerusakan. Setelah risiko telah dinilai, pembangun sistem akan berkonsentrasi pada titik kontrol dengan kerentanan terbesar dan potensi kerugian. Pada kasus ini, kontrol harus fokus pada cara-cara untuk meminimalkan risiko gangguan listrik dan user kesalahan karena diantisipasi kerugian tahunan tertinggi untuk daerah-daerah tersebut.

3. Kebijakan Pengamanan

Sebuah keamanan Kebijakan terdiri dari laporan peringkat risiko informasi, mengidentifikasi diterima tujuan keamanan, dan mengidentifikasi mekanisme untuk mencapai tujuan-tujuan ini. Kebijakan keamanan mendorong kebijakan menentukan penggunaan diterima dari perusahaan sumber informasi dan yang anggota perusahaan memiliki akses ke nya aset informasi.

Kebijakan penggunaan diterima (AUP) mendefinisikan penggunaan diterima informasi sumber daya dan komputasi peralatan perusahaan, termasuk desktop yang dan komputer laptop, perangkat nirkabel, telepon, dan internet. Kebijakan harus menjelaskan kebijakan perusahaan mengenai privasi, tanggung jawab pengguna, dan penggunaan pribadi peralatan perusahaan dan jaringan. Sebuah AUP baik mendefinisikan tindakan yang tidak dapat diterima dan dapat diterima untuk setiap pengguna dan menentukan konsekuensi bagi yang melanggar.

4. Memastikan Keberlangsungan Bisnis

Jika Anda menjalankan bisnis, Anda perlu merencanakan untuk acara, seperti listrik padam , banjir, gempa bumi, atau serangan teroris yang akan mencegah sistem informasi dan bisnis Anda dari operasi.

Kedua contoh mewakili dua profil keamanan atau pola keamanan data yang mungkin ditemukan dalam sistem tenaga. Tergantung pada aturan akses, pengguna akan memiliki batasan-batasan tertentu pada akses ke berbagai sistem, lokasi, atau data dalam sebuah organisasi.

Planning devises pemulihan berencana untuk pemulihan komputasi dan komunikasi jasa setelah mereka telah terganggu. Rencana pemulihan bencana fokus terutama pada teknis isu yang terlibat dalam menjaga sistem dan berjalan, seperti yang file untuk kembali dan pemeliharaan sistem komputer cadangan atau pemulihan bencana jasa. Manajer bisnis dan spesialis teknologi informasi perlu bekerja bersama-sama pada kedua jenis rencana untuk menentukan sistem dan bisnis proses yang paling penting untuk perusahaan. Mereka harus melakukan usaha analisis dampak untuk mengidentifikasi sistem yang paling penting perusahaan dan dampak yang sistem pemadaman akan memiliki pada bisnis. Manajemen harus menentukan jumlah maksimum waktu bisnis dapat bertahan dengan sistem yang turun dan bagian mana dari bisnis harus dipulihkan terlebih dahulu.

5. Peran Proses Audit

Sebuah audit menyeluruh bahkan akan mensimulasikan serangan atau bencana untuk menguji respon dari teknologi, staf sistem informasi, dan bisnis karyawan. Daftar audit dan peringkat semua kelemahan kontrol dan memperkirakan kemungkinan terjadinya mereka. Kemudian menilai dampak keuangan dan organisasi setiap ancaman.

D. TEKNOLOGI DAN ALAT UNTUK MELINDUNGI SUMBER INFORMASI

Bisnis memiliki berbagai teknologi untuk melindungi informasi mereka sumber. Mereka termasuk alat untuk mengelola identitas pengguna, mencegah tidak sah akses 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 mengotomatiskan proses melacak semua pengguna dan sistem hak mereka, menetapkan setiap pengguna identitas digital yang unik untuk mengakses setiap sistem. Hal ini juga mencakup perangkat untuk otentikasi pengguna, melindungi identitas pengguna, dan mengendalikan akses ke sumber daya sistem. Untuk mendapatkan akses ke sistem, pengguna harus resmi dan dikonfirmasi.

Firewall, Sistem Deteksi Gangguan, dan Antivirus Perangkat Lunak

Firewall

Firewall adalah kombinasi dari hardware dan software yang mengontrol aliran lalu lintas jaringan masuk dan keluar. Hal ini umumnya ditempatkan antara jaringan internal yang swasta organisasi dan jaringan eksternal tidak memercayai, seperti Internet, meskipun firewall juga dapat digunakan untuk melindungi satu bagian dari jaringan perusahaan dari sisa jaringan. Firewall bertindak seperti gatekeeper yang meneliti mandat masing-masing pengguna sebelum akses diberikan ke jaringan. Firewall mengidentifikasi nama, IP alamat, 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 komunikasi yang tidak sah ke dalam dan keluar dari jaringan. Dalam organisasi besar, firewall sering berada pada ditunjuk khusus komputer terpisah dari sisa jaringan, sehingga tidak ada permintaan yang masuk langsung mengakses sumber daya jaringan pribadi.

Firewall ditempatkan antara perusahaan jaringan pribadi dan Internet publik atau jaringan lain tidak mempercayai untuk melindungi terhadap lalu lintas yang tidak sah.

Untuk membuat firewall yang bagus, administrator harus menjaga rinci internal yang aturan mengidentifikasi orang, aplikasi, atau alamat yang diperbolehkan atau ditolak. Firewall dapat mencegah, tapi tidak sepenuhnya mencegah, penetrasi jaringan oleh pihak luar dan harus dipandang sebagai salah satu unsur dalam rencana keamanan secara keseluruhan.

Intrusion Detection Systems

Selain firewall, vendor keamanan komersial sekarang menyediakan intrusi alat dan layanan deteksi untuk melindungi terhadap lalu lintas jaringan yang mencurigakan dan mencoba untuk mengakses file dan database. Sistem deteksi intrusi fitur alat monitor penuh waktu ditempatkan pada titik-titik yang paling rentan atau "hot spot" dari jaringan perusahaan untuk mendeteksi dan mencegah penyusup terus. Sistem ini menghasilkan alarm jika menemukan peristiwa yang mencurigakan atau anomali.

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 sudah diketahui kapan software ditulis. Untuk tetap efektif, perangkat lunak antivirus harus terus diperbarui.

- ***Unified Threat Management Systems***

Untuk membantu bisnis mengurangi biaya dan meningkatkan pengelolaan, vendor keamanan telah digabungkan menjadi satu alat berbagai alat keamanan, termasuk firewall, jaringan pribadi virtual, sistem deteksi intrusi, dan konten Web penyaringan dan software antispam. Manajemen keamanan yang komprehensif ini disebut manajemen ancaman terpadu (UTM) sistem. Meskipun awalnya ditujukan untuk businesss kecil dan menengah, produk UTM tersedia untuk semua ukuran jaringan.

Mengamankan Jaringan Nirkabel

Langkah pertama yang sederhana untuk menggagalkan hacker adalah untuk menetapkan unik nama untuk SSID jaringan Anda dan menginstruksikan router Anda tidak menyiarkannya. Perusahaan dapat lebih meningkatkan keamanan Wi-Fi dengan menggunakannya dalam

hubungannya dengan private network (VPN) teknologi virtual ketika mengakses internal perusahaan data.

Enkripsi Dan Infrastruktur Kunci Publik

Proses Enkripsi mengubah teks biasa atau data ke dalam teks cipher yang tidak dapat dibaca oleh siapa pun selain pengirim dan penerima yang dimaksudkan. Data yang dienkripsi dengan menggunakan kode numerik rahasia, disebut kunci enkripsi, yang mengubah data yang biasa menjadi 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 Transport Layer Security penerus nya (TLS) memungkinkan klien dan server komputer untuk mengelola enkripsi dan dekripsi kegiatan mereka berkomunikasi satu sama lain selama sesi Web aman.

Memastikan Sistem Ketersediaan

Sistem komputer toleransi kegagalan mengandung hardware berlebihan, perangkat lunak, komponen dan pasokan listrik yang menciptakan lingkungan yang menyediakan terus menerus, tanpa gangguan layanan. Komputer toleran menggunakan rutin perangkat lunak khusus atau logika diri pengecekan dibangun ke sirkuit mereka untuk mendeteksi hardware kegagalan dan secara otomatis beralih ke perangkat cadangan. Bagian dari komputer ini dapat dihapus dan diperbaiki tanpa gangguan terhadap sistem komputer. Toleransi kesalahan harus dibedakan dari ketersediaan tinggi komputasi. Kedua toleransi kesalahan dan ketersediaan tinggi komputasi mencoba untuk meminimalkan downtime.

Pengendalian Jaringan Lalu Lintas: Deep Packet Inspection

DPI memeriksa file data dan memilah prioritas rendah materi online sementara menugaskan prioritas yang lebih tinggi untuk file bisnis penting. Berdasarkan prioritas didirikan oleh operator jaringan, itu memutuskan apakah sebuah paket data tertentu dapat terus tujuan atau harus diblokir atau ditunda sementara lebih hasil lalu lintas penting. Menggunakan sistem DPI dari Allot Communications, Ball State mampu untuk tutup jumlah file-sharing lalu lintas dan menetapkan itu banyak prioritas yang lebih rendah. Lalu lintas jaringan pilihan bola Negara dipercepat.

Keamanan outsourcing

Banyak perusahaan, terutama usaha kecil, kekurangan sumber daya atau keahlian untuk menyediakan lingkungan komputasi ketersediaan tinggi aman mereka sendiri. Mereka dapat

outsource banyak fungsi keamanan untuk penyedia layanan keamanan dikelola (MSSPs) yang memantau aktivitas jaringan dan melakukan kerentanan pengujian dan deteksi intrusi.

Isu Keamanan Untuk Cloud Computing Dan Mobile Digital Platform

Meskipun komputasi awan dan platform digital muncul ponsel memiliki potensi untuk memberikan manfaat yang kuat, mereka menimbulkan tantangan baru untuk sistem keamanan dan kehandalan.

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 menyelenggarakan layanan dan mengelola data yang penting. Interaktif Sesi pada detail Teknologi beberapa masalah keamanan cloud yang harus ditangani. Pengguna cloud perlu mengkonfirmasi bahwa terlepas dari mana data mereka disimpan atau ditransfer, mereka dilindungi di tingkat yang memenuhi persyaratan perusahaan mereka.

Mengamankan Platform Mobile

Jika perangkat mobile berkinerja banyak fungsi komputer, mereka perlu diamankan seperti desktop dan laptop terhadap malware, pencurian, kecelakaan kehilangan, 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 didukung, dilindungi, dan digunakan. Mereka akan membutuhkan alat untuk mengesahkan semua perangkat yang digunakan; untuk memelihara 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 bisa 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 pengguna sistem informasi departemen dan akhir untuk bersama-sama mengukur kinerja sistem dan mengidentifikasi masalah yang terjadi.

Untuk metrik untuk menjadi sukses, mereka harus hati-hati dirancang, formal, objektif, dan digunakan secara konsisten. Awal, pengujian berkala, menyeluruh dan akan memberikan kontribusi yang signifikan untuk sistem kualitas. Banyak pandangan pengujian sebagai cara untuk membuktikan kebenaran pekerjaan yang mereka miliki dilakukan. Bahkan, kita tahu bahwa semua perangkat lunak yang cukup besar yang penuh dengan kesalahan, dan kami harus menguji untuk mengungkap kesalahan ini.

Teknologi dan Alat untuk Melindungi Sumber Informasi

Management Identitas dan Otentikasi

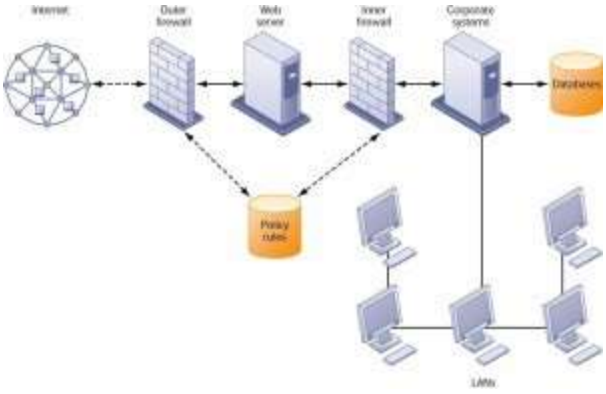
Perusahaan besar dan menengah memiliki infrastruktur TI yang kompleks dan sistem yang berbeda, masing-masing dengan mengatur sendiri pengguna. Perangkat lunak manajemen identitas mengotomatisasi proses melacak semua pengguna ini dan hak istimewa sistem mereka, menetapkan setiap pengguna identitas digital yang unik untuk mengakses setiap sistem. Hal ini juga mencakup perangkat untuk otentikasi pengguna, melindungi identitas pengguna, dan mengendalikan akses ke sumber daya sistem.

Firewall, Intrusion Detection Systems, dan Antivirus Software

Tanpa perlindungan terhadap malware dan penyusup, terhubung ke Internet akan sangat berbahaya. Firewall, sistem deteksi intrusi, dan perangkat lunak antivirus merupakan 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 masuk dan keluar.



Gambar : Firewall Perusahaan. Firewall ditempatkan antara perusahaan jaringan pribadi dan Internet publik atau jaringan lain tidak mempercayai untuk melindungi terhadap lalu lintas yang tidak sah.

Intrusion Detection Systems

Selain firewall, vendor keamanan komersial sekarang menyediakan alat-alat deteksi intrusi dan layanan untuk melindungi lalu lintas jaringan yang mencurigakan yang berupaya untuk mengakses file dan database. Sistem deteksi intrusi merupakan fitur alat pemantauan penuh waktu yang ditempatkan pada titik-titik yang paling rentan atau "hot spot" pada jaringan perusahaan untuk mendeteksi dan mencegah penyusup. Sistem ini akan menghasilkan alarm jika menemukan peristiwa atau anomali yang mencurigakan. Scanning software mencari pola untuk menunjukkan metode yang dikenal serangan komputer, seperti password yang buruk, memeriksa apakah file penting telah dihapus atau diubah, dan mengirimkan peringatan vandalisme atau sistem administrasi kesalahan.

Antivirus and Antispyware Software

Rencana teknologi defensif yang kedua untuk individu dan bisnis harus mencakup perlindungan antivirus pada setiap komputer. Perangkat lunak antivirus dirancang untuk memeriksa sistem komputer dan drive terhadap kehadiran virus komputer. Seringkali perangkat lunak menghilangkan virus dari daerah yang terinfeksi. Namun, antivirus hanya efektif terhadap virus yang sudah dikenal ketika perangkat lunak dibuat. Untuk tetap efektif, antivirus harus terus diperbarui.

Unified Threat Management System

Untuk membantu bisnis mengurangi biaya dan meningkatkan pengelolaan, vendor keamanan telah digabungkan menjadi satu kesatuan alat keamanan, termasuk firewall, jaringan pribadi virtual, sistem deteksi intrusi, dan konten Web penyaringan dan software antispam. Produk manajemen keamanan yang komprehensif ini disebut sistem manajemen ancaman terpadu (UTM). Meskipun awalnya ditujukan untuk bisnis kecil dan menengah, produk UTM tersedia untuk semua ukuran jaringan. Vendor terkemuka UTM termasuk palang, Fortinent, dan Check Point, dan vendor jaringan seperti Cisco Systems dan Juniper Networks menyediakan beberapa kemampuan UTM dalam peralatan mereka.

Mengamankan Jaringan Wireless

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

4. Enkripsi dan Infrastruktur Kunci Publik

Banyak bisnis menggunakan enkripsi untuk melindungi informasi digital yang mereka menyimpan, 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 dimaksudkan. Data yang 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 Socket Layer (SSL) dan Transport Layer Security penerus 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.

Gambar Enkripsi Kunci Publik

Sebuah sistem enkripsi kunci publik dapat dilihat sebagai rangkaian kunci publik dan swasta yang mengunci data ketika mereka ditransmisikan dan membuka data ketika mereka diterima. Pengirim menempatkan kunci publik penerima dalam sebuah direktori dan menggunakannya untuk mengenkripsi pesan. Pesan dikirim dalam bentuk terenkripsi melalui Internet atau jaringan pribadi. Ketika pesan terenkripsi tiba, penerima menggunakan kunci pribadi nya untuk mendekripsi data dan membaca pesan.

Memastikan Sistem 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.

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 pengguna sistem informasi departemen dan akhir untuk bersama-sama mengukur kinerja sistem dan mengidentifikasi masalah yang terjadi. Contoh metrik perangkat lunak meliputi jumlah transaksi yang dapat diproses di unit waktu tertentu, waktu respon online, jumlah cek gaji yang dicetak per jam, dan jumlah bug yang dikenal per seratus baris kode program. Untuk metrik menjadi sukses, mereka harus hati-hati dirancang, formal, objektif, dan digunakan secara konsisten.