Pedoman Praktis
Keamanan Informasi Organisasi
Skala Kecil Dan Menengah

Studi Kasus Serangan
Dan 12 Rekomendasi Langkah Pengamanan

Direktorat Sistem Informasi. Perangkat Lunak dan Konten
Direktorat Jendral Aplikasi telematika
Departemen Komunikasi Dan Informatika

2007

Ditertibkan Oleh **:** Direktorat Sistem Informasi,
Perangjat lunak dan Konten
Direktorat Jenderal Aplikasi Telematika
Deaprtemen Komunikasi Dan Informatika

Susunan Redaksi

Pembina **:** Cahyana Ahmadjayadi
Pengarah **:** Lolly Amalia Abdulah
Koordinator **:** Aidil Chendramata
Editor **:** Juliati Junde
NaraSumber **: -** Maeran Sunarto
- Teddy Sukardi
- Hogan Kusnadi

Cetakan Kedua, Mei 2007

SAMBUTAN
DIREKTUR JENDRAL APLIKASI TELEMATIKA

Sejalan Perkembangan Teknologi Informasi dan Komunikasi (TIK) peran TIK dalam kehidupan bangsa Indonesia meningkatkan drastis, termasuk pemanfaat TIK organisasi skala kecil dan menengah.

Sayangnya, organisasi skala kecil dan menegah yang memanfaatkan TIK, umumnza kurang memperhatikan faktor keamanan Informasi. Informasi bagi sebuah organisasi atau perusahaan merupakan salah satu aset yang sangat penting, karena kehilangan informasi dapat mengakibatkan kerugian yang tidak sedikit,

Oleh karena itu Keamanan Informasi harus mendapat perhatian, apabila tidak ingin kerugian yang lebih besar.

Direktorat Sistem Informasi, Perangkat Lunak dan Konten menyusun **'Pedoman Praktis Keamanan Informasi untuk Organisasi Skala Kecil dan Menengah'** dan diharapkan menjadi salah satu rekomendasi bagi para pelaku usaha skala kecil dan menengah dalam mengelola resiko Keamanan Informasi.

Saya menyambut baik penyususnan pedoman ini, semoga pedoman ini dapat memberikan manfaat dalam pemahaman tentang pentingnya keamanan informasi bagi para pelaku usaha skala kecil dan menengah yang memanfaatkan teknologi informasi dan komunikasi dalam menunjang bisnis mereka.

Salam Aptel

Jakarta, Desember 2006

Cahyana Ahmadjayadi

Kata Pengantar

Kesadaran para pelaku bisnis skala kecil dan menegah akan pentingnya memanfaatkan Teknologi Informasi dan Komunikasi (TIK) dalam menunjang bisnis, mulai meningkat. Hal ini terlihat dengan maraknya produk dan jasa yang mereka tawarkan melalui internet menggunakan aplikasi untuk kegiatam manajemen dan operasional. Namun, tanpa disadari pemanfaatan teknologi informasi dapat membawa dampak ancaman keamanan informasi yang cukup serius karena dapat menyebabkan kerugian yang sangat tinggi.

Keamanan informasi perlu diperhatikan tidak saja bagi organisasi atau perusahaan besar tetapi organisasi skali kecil dan menengah juga perlu memperhatikan keamanan informasinya.

Pada umumnya kurang kesadaran terhadap keamanan informasi disebabkan karena keterbatasan pengetahuan dan kamampuan Sumber Daya Manusia (SDM) serta sarana dan prasarana yang berkaitan dengan Keamanan Informasi belum memadai.

Sebagai upaya untuk mengatasi hal tersebut, Direktorat Sistem Informasi, Perangkat Lunak dan Konten menyusun **'Pedoman Praktis Keamanan Informasi untuk Organisasi Skala Kecil dan Menengah'.** Pedoman ini diadopsi dari *Common Sense Guide to Cyber Security for Small Businesses oleh Carol Woody and Larry Clinton (Internet Security Alliance)* yang diharapkan dapat membantu memberikan pemahaman tentang keamanan informasi kepada para pengusaha kecil dan menengah.

Kami menyampaikan terimakasih kepada semua pihak yang telah membantu dalam menyelesaikan buku pedoman ini.

Tak ada gading yang Tak Retak, oleh karena itu kami akan berusaha untuk terus memperbaharui dan melengkapi pedoman ini. Komentar dan tanggapan terhadaap pedoman ini sagat membantu penyempurnaan pedoman ini, sehingga diperoleh pedoman yang palinf sesuai bagi organisasi skala kecil dan menengah di Indonesia. Korespondensi ditujukan ke alamat e-mail:

Ksi_ditsiplk@depkominfo.go.id

Semoga bermanfaat!!

Jakarta, Desember 2006

Lolly Amalia Abdullah
Direktur
Sistem Informasi, Perangkat Lunak dan Konten

PENDAHULUAN

Saya sangat sibuk: Haruskah saya membaca ini ?

Ya. Banyak Pengusaha kecil dan menengah mendapat kesan yang salah tentang ukuran usahanya, atau upaya keamanan minimal yang telah mereka ambil, akan melindunginya dari serangan *cyber.*

Asumsi ini selain tidak tepat juga berbahaya.

Seramgan pada sistem informasi yang dioperasikan oleh UKM berkembang pesat dan membawa dampak serius pada operasi bisnis. Satu survey menunjukan bahwa satu dari setiap tiga UKM terkena virus *"MyDoom"* yang lalu. Ini berarti dua kali daro proporsi Perusahaan Besar yang terkena serang virus serupa.

Penyebaran serangan aninimus oleh virus popular seperti "Code red." "Blaster." Dan "So Big" telah meningkatkan publisitas karena dampak negative atas semua jenis usaha telah meningkat. Perkiraan asuransi menunjukan bahwa sampai tahun 1996 jumlah kerugian usaha karena serangan cyber mungkin kurang dari satu milyar dollar setahun. Perkiraan kerugian usaha sekarang mencapai beberapa milyar dollar setiap minggu akibat berbagai bentuk serangan cyber.

Anehnya, korporat besar lebih banyak kehilangan dalam hal kerugian jumlah dollar. Namun, semakin kecilnya margin keuntungan dimana UKM beroperasi membuatnya lebih penting bahwa mereka harus lebih pro-aktif memproteksi sistem informasinya. Bayangkan apa yang akan terjadi jika data komputer bisnis anda tidak di-backup secara regular. Bagaimana buruk dampak kehilangan bisnis komputer anda terhadap kemampuan anda berusaha secara normal kembali?

Berapa besarnya biaya untuk memperbaikinya?

Berapa banyak data yang hilang dan tidak tergantikan?

Berapa besarnya kerugian yang harus anda tanggung akibat hilangnya data ini ?

Dapatkah anda bangkit mengatasi kesulitan dan kemacetan usaha ini ?

Contohnya nyata Sehari-hari- ini dapat terjadi pada anda

Akibat satu seri serangan komputer, sebuah perusahaan yang sebelumnya bernilai $ 1 juta, sekarang harus menjual daftar pelangganya. “Bisnis saya pailit. Bisnis istri sys juga bangkrut. Sekarang saya hanya berharap masih bisa mempertahankan rumah saya,” kata mantan pemilik perusahaan dengan sedih, seperti dirujuk dalam Komputer World Magazine. Deskripsi lengkap kasus ini dapat anda lihat dalam langkah-11.

Booklet ini berisi contoh dari berbagai jenis UKM yang menanggung kerugian signifikan karena berbagai serangan cyber. Tidak semua kerugian seserius contoh di atas. Pada kenyataan beberapa perusahaan berhasil bertahan dengan baik. Namun, ini bukanlah kasus hipotetikal. Mereka adalah kejadian nyata UKM yang dilaporkan oleh media, ditanyakan dalam situs web FBI, atau dilaporkan langsung sepanjang proses riset penulisan publikasi ini.

Meskipun contoh yang termuat di seluruh buku ini, mereka tidak menggambarkan secara spesifik praktek seperti dideskripsikan. Serangan komputer tidak bekerja demikian. Sering suatu serangan merupakan kombinasi dari beberapa kesalahan. Yang menarik adalah skala bisnis yang menjadi korban secara nasional. Contoh-contoh ini mencakup manufaktur kecil, kontraktor, credit unions, hotel, rumah makan/restoran, layanan bus dan lima, perusahaan angkutan dan sekelompok professional dan konsultan termasuk firma hukum, akuntansi, dan modal ventura. Penting untuk memahami bahwa bukan besar/kecilnya usaha atau jenis bisnis, yang menjamin melindungi anda rentan terhadap serangan. Jika anda mengikuti rekomendasi pedoman yang ada di sini, secara substansiel anda akan tidak lebih rentan.

Apakah Publikasi ini cocok untuk Bisnisnya saya?

Satu analisa bahwa UKM menjadi korban serangan cyber dalam skala lebih luas dari pada perusahaan besar adalah behwa banyak perusahaan besar, dengan skala sumber dayaekonomi yang lebih baik, melakukan upaya sistematik untuk mengelola risiko pada sistem informasinya. Untuk itu mereka memiliki dan menggunakan Unit Pengelola TI yang lebih baik dari pada perusahaan kecil yang tidak mungkin dapat lakukan.

Dokumen ini dimaksud untuk para manajere non-teknis pada perusahaan yang memiliki lebih dari satu komputer, tetapi tidak memiliki unit dukungan teknis TI internal yang cukup memadai. Pengelola tunggal, dengan hanya satu komputer, lebih baik merujuk pada pedoman parkatis untuk pengguna rumah dan individual. Dokumen ini menawarkan petunjuk ekstensif untuk operasi usaha kecil.

Pedoman Praktis untuk pimpinan Organisasi didesain untuk usaha yang memiliki unit dukungan teknis internal TI yang cukup canggih. Jumlah karyayawan dan aset tahunan bukanlah criteria yang baik untuk membedakan target audiens Pedoman Praktis untuk UKM ini dengan Pedoman Praktis untuk Pimpinan Organisasi. Misalnya sebuah perusahaan konstruksi, mungkin memiliki jumlah karyawan yang banyak dan aset tahunan besar, tetapi hanya memiliki kantor pusat yang kecil dengan seorang pekerja paruh waktu (*part-time*) menangani dan menjalankan jaringan komputer.

Pedoman Praktis untuk Pimpinan Organisasi mungkin berlebihan untuk perusahaan ini. Sebaliknya, sebuah bank kecil dari pada perusahaan konstruksi hipotensi di atas, pasti lebih membutuhkan Pedoman Praktis untuk Pimpinan Organisasi, baik karena kabutuhan atau dalam kaitan dengan Pedoman Praktis untuk UKM ini, karena status legal yang kompleks dan lingkungan regulatori terkait dengan industry perbankan.

Mengapa Seseorang akan Menyerang Saya?

Banyak serangan pada Internet dan sistem jaringan tidak memiliki target spesifik.Penyerang mengirim data besar memanfaatkan suatu sistem tanpa protektif sebagai basis melancarkan serangan. Menggunakan komputer tanpa protektif firewalls, antivirus software, dan pelatihan pengguna bukan saja mempengaruhi bisnis anda, tetapi juga mempengaruhi banyak bisnis lainkarena virus menyebar di seluruh Internet.

Ketiadaan proteksi pada sistem anda menjadikan anda atau target: yang dapat merusak komputer anda, jaringan anda, dan menyumbang penyebaran virus yang memperlambat atau menghentikan sebagai dari Internet. Kita semua pengguna Internet memiliki tanggung jawab membantu menciptakan kepercayaan konsumen dan bisnis. Tetapi yang paling penting, kegagalan menerapkan best practice dapat merugikan perusahaan anda secara signifikan.

Pedoman ini member peta jalan menuju keamanan internet secara sedrhana dan mudah dipahami. Kami sarankan untuk membaca ini, menerapkannya, dan melindungi bisnis anda dan orang lain. Jangan menjadi seorang pecundang dalam konteks waktu dan uang. Jadilah seorang yang pro-aktif dari reaktif.

OK. Mungkin saya harus lakukan sesuatu, tetapi berapa besar biayanya?

Pada Desember 2003, Departemen Keamanan Dalam Negeri AS berkoordinasi dengan sektor industry menyelengarakan National Cyber Security Alliance (ISAlliance) diminta untuk menyusun publikasi best practices yang dimaksud khusus untuk usaha kecil dan menengah.

Dari pada mengerjakan berdasarkan tulisan lama, ISAlliance melakukan diskusi grup berkoordinasi dengan US Chamber of Commerce, National Association of Manufactures, National Federation of Independent Businesses, dan electronic Industries Alliance. Hampir 100 usaha kecil terlibat dalam perumusan publikasi ini, membantu mengarahkan pada kebutuhan spesifik dari komunitas usaha kecil.

Faktor biaya, baik dalam konteks waktu dan uang, adalah tema dominan dalam diskusi ini. Sebagai hasilnya, publikasi ini mencobabukan saja menyarankan langkah yang layak diambil, tetapi juga membahas isu-isu waktu, uang dan ketrampilan teknis yang diperlukan , termasuk konsekuensi yang harus ditanggung jika tidak menerapkan best practices ini. Terlebih lagi, setiap saran dirinci implementasinya atas saran praktek, bagaimana memulainya dan langkah tambahan apa yang diperlukan.

Setiap UKM memerlukan rencana keamanan selain rencana pemasaran. Anda harus segera memeriksa komponen keamanan anggaran TI anda. Sudahkah anda alokasikan anggaran yang memadai untuk keseluruhan 12 langkah yang disarankan ? jika tidak, kemudian tiba saatnya menghitung unsur-unsur yang tidak ada. Berbasis alokasi tahunan, pengeluaran anda terpusat pada software untuk pemeliharaan dan upgrade. Dalam jangka panjang, berbasis penambahan sistem, fitur keamanan yang penting perlu dialokasikan anggaran di depan baik dalam Hardware dan Software Sementara secara realidtik kita mengerti bahwa keamanan berlangsung bertahap. Adalah demi kepentingan bisnis, anda harus mengikutinya secara keseluruhan.

Bagaimana saya Bisa Tetap update, Apa yang Harus Saya Lakukan untuk Mengamankan Bisnis saya ??

Kami tidak memberikan rekomendasi vendor tertentu, karena memang di luar lingkup penyusunan pedoman ini. Kami sarankan anda menggunakan program anti-virus, misalnya, tetapi kami tidak menyarankan program dari vendor tertentu. Beberapa dari vendor mungkin melakukan tugas lebih baik dari lainnya. Pers menerbitkan tinjauaan berbagai produk mungkin ini membantu personil TI anda memutuskan menggunakan produk mana. Atau personil TI anda dapat melakukan evaluasi internal dari produk yang ada.

Kami telah mencoba berpegang pada pedoman umum yang akan terbukti dengan waktu, sehingga dokumen ini tidak menjadi cepat obsolete, sementara pada waktu yang sama mencoba untuk tetap up-to-date.

Langkah-1 : Gunakan Password yang kuat dan rubah secara regular
Biaya : Minimal-Tidak ada tambahan investasi
Tingkat keahlian teknis : Rendah sampai Medium
Peserta : Siapa saja yang menggunakan fasilitas elektronik

Mengapa harus dilakukan?

Password adalah yang paling mudah untuk membatasi akses ke lingkungan kerja elekrtonik. Password yang lebih sulit ditebak akan mencegah berbagai jenis intruder. UKM sering melakukan pergantian SDM dengan frekuensi yang lebih tinggi, yang justru labih membutuhkan perubahan password secarareguler. Karena anda tidak tahu suatu password telah bocor, rubahlah paling tidak setiap 6 bulan sekali dan mungkin 3 bulan sekali, dan jangan gunakan ulang password lama. Untuk setiap komputer dan layanan yang anda gunakan (pembelian online, misalnya), anda harus mempunyai password yang uniek.

Dengan tidak mengunakan ulang password lama, kebocoran di satu area tidak akan membuka akses ke area lain. Jangan pernah menulis password pada secarik kertas atau memberitahukan kepada siapa pun. Tetapi jika anda perlu menulisnya, simpan kertas itu di tempat yang aman seperti filing cabinetyang terkunci (tidak di bawah keyboard anda dimana seseorang mungkin akan menemukan). Setiap penguna sistem komputer harus memiliki account yang uniek dan bertanggung jawab dalam memegang psswordnya. Ini juga merupakan cara mengkaitkan aksi di jaringan kepada individual tertentu.

Password yang lemah member rasa Aman yang palsu

Tanpa membatasi akses, semua isi jarangan dapat dilihat, diubah dan dirusak siapa aja melalui akses jaringan. Jika jaringan terkoneksi ke internet (sedikit yang tidak, saat ini) informasi anda mungkin bisa diakses dari maupun di dunia. Bahkan

dengan password, perlindungan sangat terbatas. Intrude menggunakan cara trial-and-error, atau teknik brute force, untuk menemukan password. Dengan membanjiri program login dengan semua kata dalam kamus (yang memerlukan beberapa menit saja), mereka mungkin akan "menemukan" passwordnya. Jika mereka tahusesuatu tentang anda, seperti nama isteri anda jenis mobil yang anda paki, interest anda, intruder yang pintar dapat mempersempit kemungkinan password dan akan pertama mencobanya. Mereka sering berhasil. Bahkan dengan sedikit variasi, seperti menambah digit pada akhir satu kata atau mengganti huruf "o" dengan angka "0". Tidak akan banyak melindungi password dari kebocoran (misalnya, 24THErd)

Langkah Awal

Password harus dibuat kompleks sehingga tidak mudah ditebak. Jangan menggunakan kata-kata dari kamus, nama, atau variasi dari itu. Usahakan menggunakan kombinasi huruf, baik huruf besar atau kecil, nomor, dan karakter lain. Panjang password dapat bervariasi (minimum 6 karakter; lebih panjang lebih baik). Susun password mengunakan pola/pattern sehingga anda dapat mengingatkan ketika membutuhkannya tanpa harus menulisnya di atas kertas.

Biasakan karyawan untuk selalu mengubah password default dan akses inisial secepat mungkin. Kebijakan harus dibuat yang mensyaratkan password yang kuat dan mengharuskan frekuensi perubahan. Karyawan harus diberitakan betapa pentingnya password yang kuat segera setelah diangkat dan diingatkan untuk merubahnya secara regular.

Langkah-lanjutan

bangun lingkungan elektronis yang mempersyaratkan password yang kuat dengan menharuskan panjang dan struktur password yang kompleks. Terapkan prosedur perubahan password secara otomatis untuk mengendalikan kebijakan penggantian password.

Kasus 1 : Mantan karyawan mengunakan akses email lama guna memata-Matai untuk memperoleh keuntungan kompetitif.

Seseorang dari California mengaku bersalah mengakses secara illegal sistem komputer mantan majikannya dan membaca pesan email para eksekutif perusahaan tersebut dengan maksud mengambil keuntungan komersial di tempat kerjanya yang baru, sebuah perusahaan saingan.

Pihak yang bersalah adalah mantan karyawan sebuah perusahaan kontraktor di California. Setelah meninggalkan perusahaan tersebut untuk bekerja pada perusahaan lainnya, dia menggunakan akses internet ke kantor perusahaan lama untuk mengakses sistem komputer lebih dari 20 kali. Dia membaca pesan email para eksekutif perusahaan lama, mencari tahu rahasia bisnis dan meneruskan ke perusahaan baru tempatnya bekerja. Perusahaan lama menanggung kerugian dollar sebelum akhirnya FBI menghentikan aktivitasi ilegalnya.

Langkah-2 : waspadai Attachment email dan download modul internet

Biaya : Minimal tidak ada investasi tambahan
Tingkat Keahlian Teknis : Rendah sampai medium
Peserta : siapa saja yang mengunakan fasilitas elektronik

Mengapa saya harus berhati-hati?
Satu cara popular mengirim virus komputer adalah dengan menyertakannya dalam satu attachment dari suatu email atau materi yang di download dari suatu situs web. Belakangan, penyerangan semakin ahli mendapatkan buku alamat dan menyertakan virus dalam attachment yang Nampak datang dari orang yang anda kenal. Perusahaan harus memiliki kebijakan yang lain ketat tentang apa yang boleh atau tidak boleh didownload atau di buka sistem mereka.

Berbagai infirmasi via e-mail dan attachment memungkinkan kita mengirim laporan , salinan file, spredsheets, foto, cartoon, music dsb. Anda mengupdate dan mengembangkan software di komputer menggunakan sumber dari internet dan vendor mendorong pelanggan untuk menggunakan cara ini. Desainer situs web memanfaatkan fitur built-in untuk menge-check komputer anda guna

memastikan bahwa anda memiliki tool perangkat lunak yang dibutuhkan untuk mengakses konten, dan jika tidak ada, mereka akan secara otomatis melakukan instlasi untuk anda. Semuanya serba cepat, mudah dan menghindarkan anda dari banyak masalah teknologi yang terlalu rumit.

Seseorang yang menulis suatu program dapat mendistribusikan di internet melalui web atau mengirim salinannya sebagaie-mail attachment. Anda sangat tergantung pada penulis dari program yang berjalan di komputer anda. Fungdi apa saja yang anda dapat lakukan di komputer anda program ini juga dapat lakukan. Jika anda menghapus file, mengirime-mail, atau menambah dan mengurangi program , program yang anda baru pasang juga dapat melakukannya. Seorang intruder dapat melakukan hal-hal ini, tanpoa pengetahuan anda, melalui program yang baru saja anda pasang dan jalankan.

Apa yang terjadi jika saya tidak berhati-hati?

e-mail teks, attachment e-mail, download modul adalah jalan masuk untuk software berbahaya. Dengan membuka satu attachment e-mail atau menerima/memasang opsi download, program dicopy ke lingkungan teknologi anda (kadang-kadang dalam file temporer yang anda tidak dapat kenali dengan mudah) dan dapat menyerang melalui kerawanan sistem anda (lihat langkah-8) program berbahaya (malicious code) yang bermukim di komputer anda umumnya akan mencoba menyebar ke komputer lain melalui attachment e-mail yang dapat menyerang sistem mereka. Besarnya volume e-mail sendiri dapat membuat jaringan tersendat sebagai tambahan, malicious code dapat merusak dan menghapus file dan software yang berjalan dalam sistem anda.

Jika anda tidak mengambil langkah-langkah pencegahan, software untuk memata-matai penggunaan internet anda akan dimasukan ke komputer anda untuk men-trasir situs web yang anda gunakan dan laporan account akses web. Software perekam untuk menyedap, meyimpan dan sekuen tombol keyboard untuk account dan password juga juga dapat dipasang pada mesin anda.

Langkah Awal

Ajarkan kepada semua penggunaan e-mail untuk melakukan hal-hal berikut :

1. Jangan gunakan funsi “preview” untuk konten e-mail.
2. Jangan buka *attachment* yang program antivirus kenali sebagai berbahaya (lihat Langkah-3)
3. Jangan buka e-mail (hapus saja) dari seseorang yang tidak dikenali, khususnya jika baris subyeknya berisi :
   - Kosong atau berisi huruf dan angka yang tidak bermakna.
   - Member tahu anda telah memenangkan kontes yang ada tidak pernah ikut atau uang yang anda harus ambil.
   - Mendskripsikan detil produk yang mungkin anda sukai.
   - Memberitahu anda tentang masalah dengan instruksi pemasangan software di mesin anda.
   - Memeberitahu anda kesalahan tagihan atau rekening untuk suatu layanan yang anda tidak pernah gunakan.
4. Jika anda tahu pengirimnya dan memutuskan untuk membuka e-mail, periksa untuk memastikan apakah konten dengan nama *attachment* dan baris subyek masuk akal.

Langkah-lanjutan

Setup software anda untuk mengingatkan anda tehadap *download* modul internet dan tidak menerima jika datang dari situs yang tidak dikenal, terutama jika e-mail datang dari orang yang tidak anda kenal membawa anda ke situs tersebut. Hapus dan jangan teruskan e-mail berantai (serupa surat berantai) dan jangan gunakan fungsi *unsubscribe* untuk layanan yang anada tidak perah *subscribe* karena ini hanya memberitahu penyerang satu satu alamat aktif telah diidentifikasi dan menjadikan anda satu sasaran jebakan.

Non-aktifkan penggunaan *java scripting* dan *Active-X* dalam browser anda dan hanya aktifkan secara temporer untuk halaman web tertentu. Jika anda berpikir untuk membeli suatu software, cari satu dengan deskripsi yang jelas tentang program dan fitur0fiturnya serta pastikan sumber informasinya dapat dipercaya.

Kasus-2 : Worm MyDoom telah sangat merugikan ribuan UKM

E-mail worm MyDoom dan variannya menyebar dengan pesat, mencapai 30% dari semua puncak lalu-lintas e-mailpada awal pebruari 2004. Worm datang dengan camouflase *attachment* e-mail, yang, jika dibuka, dapat membuat suatu backdoor yang akan membuka akses illegal ke dalam suatu komputer, yang mungkin dimanfaatkan untuk berbagai tujuan tidak baik di waktu mendatang.
Riset menunjukan hampir 1 dari 3 UKM telah menjadi korban MyDoom disbanding 1 dari 6 korporat besar. Lebih jauh, *MyDoom* dapat menyebar melalui jaringan *file sharing* seperti *kazaa.* Jumlah kerugian sebagai akibat *MyDoom* sudah mencapai beberapa milyar dollar dan masih terus bertambah.

Langkah-3 : Pasang. Pelihara dan Terapkan Program Anti-Virus

Biaya : Rendah – Tersedia lisensi Situs
Tingkat Keahlian Teknis : Rendah sampai medium tergantung cara pendekatan
Peserta : Semua yang menggunakan fasilitas elektronik

Mengapa harus melakukannya??
Program anti-virus adalah cara murah melindungi sistem dan informasi anda dari ancaman eksternal. Virus (program berbahaya yang tersembunyi dalam file) memanfaatkan kerawanan lingkungan teknologi, dan jumlah kerawanan yang teridentifikasi berlipat dua setiap tahunnya sejak pelaporan dilakukan pada 1988. Kerwanan terdapat pada stiap aspek hardware dan software yang ada di pasar saat ini. Virus paling dikenal dikirim melalui *attachment* e-mail, dan infeksi terjadi ketika *attachment* dibuka (lihat langkah-2)

Virus dapat menginfeksi sebuah komputer dalam berbagai cara : melalui Floppy disks, CD, e-mail, situs web, dan files yang di-*download.* Ketika anda membaca sebuah floppy disk, menerima e-mail, atau download sebuah file, ada perlu periksa adanya virus. Program anti-virus (AV) melihat isi dari setiap file, mencari karakter spesifikasi yang memiliki profil atau pattern-disebut virus signature-yang dikenal berbahaya. Untuk setiap file yang memiliki kesamaan dengan sebuah

signature, satu program AV member beberapa opsi, sperti menghapus pattern penyerangan atau menghancurkan file atau *attachment* e-mail yang berisi virus. Ketika *vendor* program AV menemukan satu virus baru, mereka meng-update *virus signature* yang dipasang pada setiap mesin untuk memeriksa kemungkinan masalah baru. Opsi update otomatis dapat diaktifkan untuk setiap mesin.

Apa yang terjadi tanpa proteksi Anti-Virus

Intruders umumnya paling berhasil menyerang setiap komputer ketika mereka mengunakan virus sebagai cara untuk mendapatkan akses. Memasang sebuah program AV dan menjaganya tetap up-to-date, diantaranya adalah suatu cara pertahanan terbaik. Ketika suatu mesin terinfeksi, software dapat menjadi tidak berfungsi dan data rusak, dan mesin tersebut akan mencoba menginfeksi mesin-mesin lainnya, memenuhi *bandwidth* komunikasi yang tersedia, menghambat jaringan dan *overload* server. Perlindungan diperlukan untuk setiap mesin.

Langkah Awal

Pasang program anti-virus pada setiap mesin dan jaga file *signature up-to-date* melalui update otomatis setiap tahunnya seperti diperlukan untuk memelihara file *virus signature* up-to-date pada mesin stiap mesin.

Jangan sekali-kali koneksi ke internet tanpa mengaktifkan program AV terlebih dahulu. Tanmkan kepada semua pengguna komputer untuk menghapus atau menghancurkan file yang teridentifikasi terinfeksi oelh program AV. Pastikan mereka tahu bagaimana melepas mesin dari jaringan dan siapa harus dipanggil jika mereka curiga mesinnya terinfeksi.

Beritahu semua pengguna e-mail untuk tidak membuka *attachment* e-mail dari sumber yang tidak diharapkan atai tidak dikenal (lihat langkah-2) untyuk menvegah penyebaran virus baru yang belum dapat diidentifikasi program AV.

Langkah lanjutan

Aktifkan program AV untuk secara otomatis memeriksa asal setiap file pada setiap mesin ketika digunakan (CD, floppy, etc). jadwalkan pemeriksaan AV periodic

semua file secara regular, sebaiknya setiap minggu, untuk menemukan masalah yang mungkin terlewati pada pemeriksaan lain.

Kasus-3 : Konsultan tidak meng-update Software; akhrinya terinfeksi dan kehilanggan pelanggan

seorang konsultan utilitas beroperasi sebagai praktisi tunggal membeli sebuah komputer baru untuk mengelola bisnisnya yang sedang berkembang. Si penjual memberitagu komputernya telah dipasang dengan aplikasi antivirus. Celakanya, si konsultan tidak menyadari bahwa dia perlu mengup-date program anti-virusnya, sistemnya terinfeksi.

Buku alamatnya dimanfaatkan untuk menyebar virus kapada para pelanggan melalui e-mail palsu, membawa akibat beberapa pelangganya memutuskan hubungan bisnisnya denganya bisnis dengannya.

Langkah-4 : Pasang dan Gunakan sebuah Firewall

Biaya : Moderat-software gratis tetapi penyesuaian efektif cukup makan waktu.
Tingkat Keahlian Teknis : Moderat sampai tinggi tergantung cara pendekatan
Peserta : Bagian Teknis

Mengapa Harus Melakukannya??

Suatu firewall banyak berfungsi seperti seorang panjaga keamanan di suatu gedung umum. Firewall memeriksa pesan yang datang kedalam sistem anda dari internet, juga pesan yang anda kirim keluar. Firewall menentukan jika pesan-pesan ini dapat di teruskan ke tujuan atau harus dihentikan. Firewall “penjaga” dapat sangat mengurangi volume pesan yang tidak dikehendaki dan berbahaya masuk ke dalam jaringan anda, tetapi perlu upayaa dan waktu untuk membangun dan memeliharanya. Firewall juga dapat mencegah berbagai bentuk akses yang tidak dikehendaki ke jaringan anda.

Bagian paling sulit adalah merumuskan aturan-apa yang diperbolehkan masuk atau keluar dari sistem anda. Jika anda tidak mengijinkan apapun masuk atau keluar (strategi firewall *deny-all*), komunikasi anda dengan internet sama sekali terputus. Karena ini bukanlah hal yang dikehendaki oleh perusahan, diperlukan kerja ekstra untuk ini. Beberapa bentuk firewall memberi kemudahanuntuk memeriksa setiap pesan informasi (packet) sehingga anda dapat memutuskan apa yang harus dilakukan dengannya. Jika anda hendak membeli firewall, cari fitur ini karena sangat bermanfaat. Pada hakekatnya, tidaklah mudah untuk menentukan lalu lintas informasi mana yang dapat di terima dan mana yang tidak. Cari bantuan teknik (Lihat langkah-12) untuk membantu anda mengidentifikasi penggunaan normal untuk organisasi anda dan menetapkan aturan untuk memblokir untuk lalu-lintas jaringan yang lain. Firewalls juga dapat digunakan untuk menerapkan kebijakan penggunaan sistem yang akseptable dengan seperti situs pornografi dan perjudian.

Apa yang terjadi tanpa firewall?

Tanpa ada sesuatu untuk menyaring informasi yang masuk dan keluar dari jaringan anda, anda akan sangat tergantung pada setiap pengguna individual untuk menerapkan kebiasaan *good e-mai* dan *download* (lihat langkah-2) untuk melindungi jaringan dari virus dan worm. Jika anda menggunakan koneksi internet berkecepatan tinggi seperti DSL atau modem kabel, anda juga tergantung pada pelanggan lain untuk layanan anda. Tanpa firewall, penyerang potensial dapat dengan cepat memeriksa (*Sceutinize*) setiap komputer yang ada dalam jaringan untuk menemukan kerawanan (lihat langkah-8) dan menyerang.

Langkah Awal

Pasaang satu firewall individual pada setiap mesin dan setup untuk memblokir lalu lintas semua layanan kecuali yang secara spesifikasi diperuntukan pada mesin tersebut (Linhat langkah-5). Tanamkan pada para karyawan anda akan nilai dari firewall sehingga mereka akan ikut membantu memperbaiki aturan, dari pada menonaktifkannya ketika proses perumusan, mungkin terjadi hal-hal seperti *over-blocking,* yang membuat operasi beberapa layanan komputer menjadi sulit.

Langkah Lanjutan

Dapatkan bantuan teknik untuk memasng satu atau lebih firewall untuk jaringan anda sesuai konfigurasi sistem. Rumuskan satu kebijakan keamanan untuk dilaksankan dengan aturan dalam firewall yang akan menentukan apa yang dikehendaki atau tidak dikehendaki dalam jaringan. Lakukan juga proses penyesuaian kebijakan keamanan untuk satu pengecualian yang disepakati beritahu karyawan akan nilai dari suatu solusi menyeluruh dan bangun mekanisme untuk memonitor dan merubah aturan sesuai perkembangan sesuai kebutuhan organisasi.

Kasus-4 : Hotel dan Koneksi Wireles internet membutuhkan Firewall

"Umumnya hotel menawarkan layan *secure broadband,* tetapi tidak cukup tahu isi-isi keaman untuk menyampaikan pertanyaan kepada penyediaan layanan," seorang pakar broadband mengatakan kepada CNN. "seorang tamu Daru perusahaan A dapat masuk ke dalam satu konperensi perusahaan B pesangannya, yang mencuri informasi korporat berharga dan memberikan hotel menanggung kemungkinan tuntuan kerugian," CNN melaporkan.

Banyak laptop memiliki setting *default* yang memungkinkan seseorang berbagi file dengan kompetre lai. Kecuali ini ditutup, *hackers* akan dapat dengan mudah masuk ketika seseorang log-in ke jaringan wireless. Firewall pribadi dapat digunakan untuk mencegah terjadinya hal ini. Semua ini berbasis *software* dan versi yang sederhana dapat di-*download* gratis on-line.

Langkah-5 : hapus software dan account pengguna yang tidak digunakan; Bersihkan semua peralatan yang di ganti

Biaya : minimal-Tidak ada investasi tambahan
Tingkat keahlian teknik : Rendah sampai medium
Peserta : Bagian teknik

Mengapa harus melakukannya?

Sistem komputer diciptakan dengan opsi tak terhingga, banyak diantaranya tidak pernah anda gunakan. Juga, proses instalasi didesain untuk kemudahan dan bukan keamanan, maka fungsi-fungsi yang menjadi masalah keamanan sering diaktifkan, seperti *remote file sharing*. Software yang tidak lagi digunakan tidak akan dipelihara dan karenanya harus dihapuskan dari sistem sehingga tidak dapat digunakan oleh penyerang sebagai sarana untuk merusak sistem anda.

Setiap pengguna komputer harus memiliki account yang uniek yang membatasi akses ke data dan software yang mereka gunakan untuk melakukan tugas (lihat langkah-1). Ketika mereka meninggalkan pekerjaan atau bergantian fungsi, kapabilitas akses perlu dihapus atau disesuaikan untuk memenuhi tugas baru. Standar teknik penggelola, seperti pemisahan tugas, perlu diterapkan dalam suatu lingkungan elektronik untuk membatasi risiko bahwa seseorang dapat menyebabkan kerugian pada bisnis anda.

Satu volume data yang besar dapat disimpan pada satu *disk drive,* dan informasi ini tetap ada ketika file dihapus. Data lain disimpan dalam file temporer yang dugunakan oleg program pada komputer. Siapa saja dapat me-retrieve informasi ini dengan mengakses disk dengan komputer lain. Untuk peralatan yang dig anti dan di rubah peruntukan, dibuang, diberikan atai dijual, disk space harus dihapus (overwrite) untuk mencegah bocornya data konfidensial atau sensitive.

Jika tidak mengganggu, tidak dapatkah saya biarkan saja?

Program dan account pengguna yang tidak digunakan berfungsi seperti buku penampung debu di atas meja . masing-masing berpotensi menjadi sarana bagi penyerang untuk mendapat akses masuk ke dalam sistem. Dengan akses masuk tersebut penyerang dapat mengambil informasi konfidensial seperti kartu kredit dan nama pelanggan, file yang cacad atau rusak dan program. Penyerang juga dapat menggunakan sistem anda sebagai basis untuk menyerang sistem ini, dan korban dapat menuntut anda atas kerugian mereka. Kendali terhadap akses sistem computing perlu dikelola sebagaimana uang tunai karena kehilangan informasi penting dapat sangat berbahaya bagi bisnis spsrti halnya uang. Jiak

account yang tidak digunkan tersebut milik mantan karyawan, mereka akan dapat terus mengakses kebisnis anda dan mencuri atau merusak informasi konfidensial dengan terus menggunakan akses mereka ke sistem. Jika anda meng-upgrade peralatan, data yang tersimpan pada peralatan yang diganti tidak hilang. *Software utility* tersedia untuk membaca file yang sudah dihapus dan informasi dari disk yang telah di-reformat.

Langkah Awal

Hapus account mentan karyawan ketika mereka berhenti. Ketika memecat seseorang, hapus akses komputernya sebelum memberitahu pemecat mereka dan lakukan pengawasan selama mereka masih dilingkungan perusahaan. Buat kebijakan bahwa software yang tidak diperlukan tidak dipasang pada komputer perusahaan (seperti games, software gratis, music dsb). Buat suatu prosedur untuk menghapus data pada semua hard driver komputer ketika peralatan dirubah peruntukannya, dibuang, didonasikan atau dijual. Gunakan program *utility* untuk menghapus semua informasi pada *hard disk* dengan *over-write.*

Langkah-lanjutan

Uninstall software dan *archive* data file arsip yang sudah tidak digunakan lagi. Semakin sedikit *clluter* data pada sistem anda, semakin mudah mengelola*backups* (lihat Langkah-7) dan menjaga level update software dalam sistem (lihat Langkah-8).

Meski mungkin membantu, adalah sangat beresiko untuk mempercaya sistem pada setup *default vendor.* Fungsi *default* merupakan target yang rawan bagi penyerang-dan kemungkinan sangat tinggi karena pemasang umumnya memilih setup sistem *default.* Kurangi potensi menjadi target dengan secara eksplisit memilih fungsi-fungsikomputer yang anda perlukan pada waktu instalasi. Jika anda tidak tahu apa fungsi itu, minta bantuan informasi dan pastikan itu sesuatu yang memang anda perlukan sebelum memasangnya. Sedikit berhati-hati pada wawl pemasangan, akan mencegah anda dari masalah besar kemudian.

Kasus-5 : Sebuah UKM Konsultan Telecom Kehilangan potensi Bisnis ketika Kebocoran Keamanan diketahui Calon Pelanggan

Sebuahperusahaan konsultan telekomunikasi dengan 8-10 karyawan berhasil menjalin perjanjian bisnis dengan sebuah konsultan keamanan untuk suatu proye bersama. Untuk memastikan, konsultan keamanan mengirim surat ke pimpinan perusahan melalui e-mail, yang tidak pernah diterima.
Sebaliknya, konsultan tersebut menerima nota kembali bersama e-mail aslinya yang berbunya "Jangan melakukan bisnis dengan perusahaan ini kami adalah aparat pemerintah dari DEA dan FBI. Email ini telah dikirim kepada anda secara konfidensial, jika anda membuka informasi ini kami akan menuntut anda." Karena konsultan bekerja dibidang keamanan, dia menganggap nahwa peringatan ini palsu dan mengkontak kantor kejaksaan dan FBI.
Konsultan tersebut juga memutuskan perjanjian dengan perusahaan telekomunikasi, yang mengancam akan menuntutnya, suatu ancaman yang tidak pernah dilaksankan, akhirnya diketahui bahwa e-mail palsu dikirim oleh mantan karyawan yang membangun sistem e-mail perusahaan telekomunikasi tersebut. Sebelum keluar meninggalkan perusahaan, dia mengature agar semua e-mail ke pimpinan perusahaan di-forward langsung kepadanya. Yang bersangkutan tidak pernah dibawa kepengadilan.

Langkah-6 : Bangun kendali akses fisik untuk semua peralatan komputer

Biaya: minimal
Tingkat keahlian teknik: Rendah sampai medium
Peserta: Siapa saja yang menggunakan fasilitas elektronik

Mengapa Harus Malakukanya??
Bagaimana bagus passwords (lihat Langkah-1) dan control keamanan pada komputer, laptop, atau PDA, jika seseorang memiliki akses fisik terhadapnya mereka akan dapat menerobos keamanan dan penggunaanya atau seharusnya ditinggal tanpa pengawasan di dalam atau di luar kantor, terutama ketika seorang pengguna sedang log on dan aktif.
Staf kebersihan dan pemeliharaan, pengunjung dan anggota keluarga karyawan dapat men-download pogram berbahaya (lihat Langkah-2) atau secara tidak sengaja merubah atau merusak file dan program ketika menggunakan komputer.

Mengunci peralatan ke meja atau dinding bukanlah perlindungan yang cukup untuk data atau software yang tersimpan di dalamnya. Jika akses jaringan (disebut notwork drops) adalah aktif di area terbuka seperti kantor yang kosong, ruang konperensi, seseorang dapat menyambung suatu peralatan suatu peralatan untuk menerobos jaringan.

Kehilangan kendali fisik adalah kehilangan keamanan

Siapapun dengan akses fisik ke suatu peralatan elektronik termasuk repairmen, bagian teknik, dan anggota keluarga, dapat menerobos instalasi control dan melihat, merubah, dan merusak data dan program pada komputer anda, jika peralatan anda terkoneksi ke jaringan, data dan program pada komputer lain dalam jaringan juga berisiko. Pemasangan suatu control akan memperlambat mereka tetapi tidak akan menghentikannya, serupa dengan poteksi oleh kunci pintu terhadap pencuri yang ahli.

Langkah Awal

Tetapkan kebijakan penggunaan normatif karyawan yang mengharuskan:

1. *Logging off* atau pengaktifan *screen lock* untuk komputer mereka sebelum meninggalkannya tak terjaga, bahkan untuk waktu yang singkat
2. Memberikan tanggungjawab kepada karyawan terhadap akses komputer dan peralatan yang bawa keluar lingkungan kerja
3. Membatasi penggunaan pribadi komputer kantor kepada karyawan dan anggota keluarganya
4. Membatasi penggunaan peralatan pribadi pada jaringan perusahaan
5. Menetapkan ancaman hukuman terhadap pelanggran aturan penggunaan peralatan secara pribadi

Pastikan semua peralatan diproteksi dari lonjakan tegangan listrik dengan stabilizer. Kunci peralatan yang terletak dalam area dengan lalu-lintas tinggi. Simpan peralatan yang tidak digunakan dalam area terkunci dan atur proses *sign-ot* melalui individu yang bertanggungjaeab atas kunci. Didiklah karyawan tentang kebijakan dan lakukan pemerikjsaan bahwa kebijakan diikutiu dengan baik.

Langkah-Lanjutan

Dapatkan bantuan teknik untuk menerapkan otentikasi semua perangkat *portable* terkoneksi kembali jaringan. Kunci ruangan kantor kosong dan konperensi di mana sambungan akses jaringan aktif berada ketika tidak dugunakan. Tinjau kontrak dukungan teknik dan layanan perbaikan dengan memasukan jaminan (*liability*) untuk peralatan dan informasi di dalamnya yang diserahkan untuk perbaikan.

Kasus-6 : Perusahaan akutansi membuat copy fisik dan elektronik-tetapi bisnis terancam kebakaran

Satu perusahaan akutansi berkantor di sebuah gedung bersama dengan sebuah perusahaan angkutan kecil . perusahaan akutansi dengan baik membuat back up elektronik dari laporan pajak (*tax return*) pelanggannya dan menyimpan copy fisik dalam filing cabinet bersama dokumen-dokumen penting lainnya. Dia juga mengatur dengan perusahaan akutansi lain untuk menyimpan copy dari masing-masing arsip fisiknya. Namun demikian, dia berhasil mempertahankan bisnisnya hanya karena dia juga menyimpan copy arsipnya ditempat lain.

Langkah-7 : buat backups dari file, folder dan software penting.

Biaya : moderat sampai mahal (tergantung tingkat otomasi dan kecanggihan peralatan yang dipergunakan)
Tingkat Keahlian Telnik : Medium sampai tinggi
Peserta : Bagian Teknik dan Pengguna jika harus menanggani backup secara individual

Mengapa harus malakukannya?
Jika seorang *Intruder* berhasil masuk ke sistem komputer anda atau merusak program. File dan folder dalam sistem, dapatkah anda terus menjalankan bisnis anda secara efektif? Apakah jaminan asuransi anda akan mengganti beberapa hari kerugian bisnis ketika sistem komputer anda diperbaiki dan informasi dipulihkan secara manual? Banyak polis asuransi umum tidak lagi menggati kerugian karena kecelakaan *cyber* . backup adalah bentuk lain asuransi untuk membantu

memulihkan bisnis kembali ketika *intruder* menyerang atau bencana seperti kebakaran atau banjir merusak lingkungan dan aset teknologi anda.
Meng-copy fil, folder, dan program dalam berbagai bentuk media lain (seperti disk atau CD) memberikan jaminan pemulihan jika dibutuhkan. Membuat copy secara manual adalah sangat tidak praktis, selain opsi otomatis juga tersedia. Anda mungkin sudah memiliki beberapa copy dalam bentuk lain, seperti program software yang dipasang dari CD.

Backup harus dibuat setiap saat ada prubahan terhadap konten aselinya. Pilih opsi backup berdasarkan pada biaya (baik waktu dan peralatan), waktu yang terpakai untuk membuat backup, dan waktu yang dipakai untuk memulihkan kondisi aseli dari copy backup. Copy akan dibuat dalam bentuk media portable apa saja termasuk floppy disk, CD, *ZIP*Disks, atau *disk drive* portable. Teknik *mirroring* dapat dibangun untuk secara kontinyu membuat duplikasi pada waktu yang bersamaan dengan aselinya untuk pemulihan segera. Copy backup harus disimpan dilokasi aman. Sebaiknya ketempat yang berbeda untuk mencegah kehilangan akibat bencana yang sama dengan aselinya. Control fisik terhadap backups adalah sama penting dengan aselinya (lihat Practice 6)

Jika Backup tidak tersedia

Karena tidak ada proteksi yang member yang memberikan menjamin 100%, kemungkinan besar *intruder* akan berhasil menyerang dan merusak lingkungan dan aset teknologi anda atau bentuk bencana lain menghancurkan sebagian dari aset tersebut. Tanpa mekanisme pemulihan, rekonstruksi akan memakan waktu panjang dan melumpuhkan bisnis. Bahlan dengan backup, proses pemilihan tetap menjadi suatu tantangan, tetapi paling tidak ini masih dimungkinkan.

Langkah Awal

Backup semua file secara periodic sesuai skedul yang ditetapkan. Untuk memilih frekuensi backup yang memadai, perlu diingat bahwa perubahan data aseli antara waktu pembuatan backup dan kehilangan data harus dilakukan secara manual.

Pelihara backup sepanjang periode waktu untuk memungkinkan perbaikan masalah yang tidak diketemukan seketika. Backup khusus untuk tahun kalender atau tahun fiscal perlu disimpan beberapa tahun. Secara berkala periksa proses backup dan akurasinya dengan memuluhkan konten ke suatu lokasi alternatif.

Langkah lanjutan

Dapatkan bantuan teknik (lihat Langkah-12) untuk mengotomatiskan sebanyak mungkin proses backup normal untuk memastikan itu selalu terjadi. Pastikan proses backup dengan log tanggal dan waktu sehingga konten dari backup dapat divalidasi. Buat copy pada pada berbagai media (copy *fileserver* dan *copy disk portable*) untuk memberikan sebanyak mungkin fleksibilitasi pemulihan. Pastikan bahwa proses otomatis terjadi secara periodic memulihkan konten dan memverifikasi akurasinya. Periksa polis asuransi untuk memastikan bahwa data dan sistem informasi serta hak inteltual anda dijamin seperti halnya properties fisik anda

Kasus-7 : Sebuah Usaha Manufaktur kecil kehilangan Kontrak Besar
Kehilangan Kontrak Besar Pemerintah akibat serangan program"Time Bomb"

Sebuah usaha manufaktur mendapat kontrak beberapa juta doolar untuk membuat divasi pengukuran dan instrumentasi untuk NASA dan US Navy. Namun, seorang pekerja shift pagi tidak dapat logon ke sistem operasi, sebaliknya mendapat pesan bahwa sistem sedang dalam perbaikan. Tidak lama kemudian, server perusahaan *crashed,* menghancurkan semua peralatan pabrik dan program manufacturing. Ketika manajaer mencari tape backup, dia ketemukan telah hilang dan terminal kerja individual juga telah musnah.

CFO perusahaan bersaksi bahwa serangan program *Time Bom* telah menghancurkan semua program dan pembangkitan program yang memungkinkan perusahaan meng-*customize* produk mereka dan dengan demikian menghemat biaya. Akibatnya perusahaan merugu jutaan dollar, dikeluarkan dari posisinya dalam industry, dan akhirnya harus memberhentikan 80orang pekerjanya. Perusaahan dapat sedikit merasa lega bahwa pada akhrinya pihak yang bertanggungjawab/bersalah ditangkap dan dihukum.

Langkah-8 : Lakukan Update Software secara rating

Biaya : Moderat-biaya pemeliharaan software dan biaya staff untuk memasang dan memverivikasi

Tingkat Keahlian Teknik : Medium sampai Tinggi

Peserta : Bagian Teknik

Mengapa Harus Malakukannya?

Vendor software secara rutin menyediakan update (juga disebut *patches)* untuk memperbaiki maslah dan meningkatkan fungsional produk mereka. Sebagai tambahan, banyak dari pacth ini memperbaiki karawanan yang dapat digunakan oleh virus dan serangan lain untuk merusak komputer anda dan isinya. Dengan menjaga software tetap up-to-date, malfungsi software dan potensi bobolnya sistem diperkecil.

Vendor sering memberikan patch gratis melalui download dari situs web mereka. Vendor software memberikan layanan jenis recall, serupa dengan menerima notifikasi recall mobil anda. Anda dapat menerima notifikasi patch melalui e-mail dengan berlangganan pada milis yang dioperasikan oleh vendor. Melalui jenis layanan ini, anda dapat belajar tentang potensi masalah sebelum terjadi dan harapannya , sebelum intruder memperoleh kesempatan untuk memanfaatkannya. Kadang-kadang suatu patch memperbaiki suatu masalah tetapi meneyebabkan masalah lain. Ketika ini terjadi, siklus perbaikan mungkin harus diulang sampai beberapa kali patch menyelesaikan masalah secara menyeluruh.

Jika Patch tidak dilakukan

Software didistribusikan bukannya tanpa cacad. Vendor mempercayakan pada customer untuk memberitahu ketika sesuatu yang tidak diharapkan terjadi ketika software dipergunakan. Dengan tidak melakuka patches, anada kehilangan layanan perbaikan terhadap masalah yang diketemukan customer lain.

Cacad dalam pemrograman membuat software anda rawan terhadap serangan program berbahaya (malicious code) serangan ini dapat merusak dan

menghilangkan files dan menghapus mekanisme perlindungan seperti program antivirus (lihat Langkah-3) dan firewall (lihat Langkah-4) serta menambah karawanan di masa mendatang. Penyerang dapat menggunakan komputer anda sebagai basis untuk mem-bombardir komputer lain dengan e-mail yang tidak diinginkan yang Nampak datang dari anda. Intruders menemukan karawanan sebagaimana anda menemukannya-dengan memonitor daftar e-mail dan berlangganan pada layanan notifikasi otomatis. Semakin panjang daftar kerawanan diketahui, semakin besar kemungkinan seorang intruder akan menemukannya pada sistem anda dan memenfaatkannya.

Langkah Awal

Ketika anada membli suatau program, lihat apakah vendor memberikan updates. Perhatikan bagaimana vendor member jawaban atas pertanyaan tentang masalah-masalah dengan produknya. Pertimbangkan membeli jaminan garansi ekstra, jika ada. Jika patch tidak diberikan, cari tahu ketika rilis baru dikeluarkan dan pertimbangkan meng-upgrade jika perbaikan kerawan diberikan.

Cari dan lakukan update software dari vendor, terutama patch untuk kerawanam yang sudah diketahui, sesegera mungkin. Logon ke situs web vendor untuk melihat bagaimana mendapat notofikasi e-mail tepaty waktu patch. Coba berlangganan milis vendor untuk notifikasi kerawanan dan perbaikan.

Langkah-lanjutan

Bebrapa vendor memberikan program yang secra otomatis meng-kontak situs web vendor untuk mencari patches baru untuk software mereka. Program ini dapat memberitahu anada katiga patch sudah ada, dan dapat download dan men-setupnya. Anada sesuaikan memeberitahu bahwa patch baru telah keluar dan member anda opsi download dan memasngnya, jika anda menemukan kerawan dan belum ada patch tersedia, pertimbangkan menggunakan program lain sampai program aseli berhasil diperbaiki.

Kaus-8 : Layanan logistic rumah Makan Terputus, Sitem Reservasi sebuah Penginapan Crashed, karena gagal melakukan Update.

Beberapa rumah makan yang mempercayakan pada e-mail dalam urusan dengan supplier-nya, terputus layan logistiknya selama 4-hari kerangan serangan virus. Meskipun telah mencoba download patches untuk mengatasi maslahnya, ternyata tidak banyak bermanfaat karena tidak melakukan patches untuk masalh software versi sebelumnya.
Demikian pula, sebuah penginapan di North Carolina menemukan tidak dapat melakukan perbaikan pada sistemnya untuk merespons suatu serangan karena tidak mengikuti skedul pemeliharaan secara rutin. Diketemukan sistem reservasi online-nya terputus untuk beberapa hari komputernya karena khawatir juga mengalami malfungsi.

Langkah-9 : Terapkan Keamanan Jaringan Dengan Kontrol Akses

Biaya : Moderat samapi tinggi tergantung opsi yang dipilih
Tingkat Keahlian Teknik : Moderat sampai Tinggi
Peserta : Bagian Tekni dan semua pengguna jaringan

Mengapa Harus Melakukannya?
Meski lingkungan teknologi organisasi anda disebut sebagai “jaringan”, pada kenyataannya ia dalah kumpulan dari komponen yang disusun sdemikian untuk memenuhi kebutuhan teknologi spesifikasi dari organisasi. Keamanan jaringan yang baik memerlukan proteksi akses untuk setiap komponen dalam jaringan termasuk firewall (lihat Langkah-4), routers, switches, dan semua perangkat yang tersambung ke jaringan. Sebaliknya, siapa saja yang dapat masuk ke jaringan anda dapat menemukan dan memanfdaatkan komponen dan layan jringan, sebagai tambahan , remote device dan portable harus diminta otentikasinya ke jaringan untuk membatsi siapa dapat melihat dan mengakses layanan jaringan seperti basis data, file dan printer yang dipakai bersama.

Suatu firewall (lihat Langkah-4) merupakan biffer antara komponen-komponen jaringan anda dengan lingkungan eksternal. Teknik lain, seperti server proxy dan network address translation (NAT) member proteksi lebih dalam membatasi informasi mana seorang pengguna eksternal dapat tahu tentang komponen-

komponen dalam lingkungan jaringan, membuat lebih sulit bagi akses yang anda dapat pasang menggunakan kapasitas blocking dan firewall dan layanan serupa lainnya, semakin mudah untuk membuatnya aman.

Pertimbangkan Khusus

Kontrol akses yang baik sangat kritis untuk akses wireless karena pengguna jenis konektisitas ini agak kurang lebih terlihat secara fisik. Bukan tidak biasa untuk seseorang di dalam mobil di tempat parkir, mengakses suatu jaringan wireless (tanpa proteksi) dan membahayakan siapa saja dalam jaringan. Anda mungkin memiliki satu koneksi wireless atau akses rumit (dail-in) kejaringan dan tidak menyadarinya, karena banyak vendor memasangnya untuk dapat memberikan kapasitas dukungan rumit. Perangkat pamasaran dan inventori berkomunikasi ke server sentral melalui wireless (nirkabel).

Kemampuan untuk mencapai dan menggunakan layanan jaringan anda dari luar (disebut akses rumit) sangat berharga bagi karyawan, suppliers dan customer yang sering berpergian. Akses rumit juga memungkinkan vendor teknologi untuk memberikan dukungan layanan jaringan kritis secara cepat tanpa harus mengunjungi tempat anda. Karyawan dapat dan menambahkan perangkat akses rumit (dial-in) langsung ke komputer mereka agar mereka dapat bekerja dari luar.

Penggunaan jenis aksen rumit ini memerlukan kehati-hatian, atau siapa saja yang kebetulan menemukan titik akses menggunakan peralatan scanner sederhana dapat masuk menerobos jaringan atau merusak informasi. Kapasitas instant messaging, chat sessions, dan music-sharing membangun rute lain (peer-to-perr) ke dalam jaringan, menerobos banyak mekanisme keamanan tradisional suatu jaringan. Opsi-opsi ini telah berkembang menjadi akses masuk program berbahaya (malicious software) dan harus dugunak secara hati-hsecurity

Apa yang terjadi tanpa Keamanan Jaringan yang baik ??

Penyerangan terus-menerus membombardir komponen yang dapat diakses dari internet dengan queries untuk mencari kelemahan. Perangkat tanpa proteksi akan dapat doterobos dalam hitungan menit setelah diperoleh koneksi khususnya

ketika akses internet tersedia dengan modem kabel, Digital Subscriber Line (DSL), atau koneksi berkecepatan tinggi lain. Satu perangkat yang dapat ditembus menyebabkan semua perangkat jaringan lain beresiko karna dapat digunakan sebagai satu basis internal untuk mencari kelemahan dan menyerang komponen lain dalam jaringan.

Tidak semua penyerang berasal dari luar organisasi. Karyawan dapat membahayakan komputer komputer karyawan lain menggunakan peralatan (tools) yang tersedia dari internet jika keamanan jaringan kurang baik. Peralatan ini memungkinkan untuk bidang tugasnya menguntit dan menggangu pihak lain, dan menanamkan konten berbahaya pada komputer lain.

Langkah Awal

Akses ke setiap komponen dari jaringan harus di batasi untuk melindunginya dari akses yang tidak benar dan bahaya. Perlindungan dasar akses dapat dilakukan menggunakan password yang kuat (lihat Langkah-1). Tetapkan prosedur untuk tidak mengaktifkan fitur pemakaian bersama file dan printer dari setiap komputer (lihat Langkah-5) kecuali digunakan, terutama ketika mengakses internet menggunakan modem kabel, DSL, atau koneksi berkecepatan tinggi lain. Instruksikan karyawan untuk menghentikan sambungan dari internet dengan memutus sesi online dan mematikan komputer ketika tidak sedang digunakan.

Akses ke perangkat proteksi jaringan seperti firewall (lihat langkah-4), switches, dan routers harus dibatasi hanya kapada individu yang bertanggung-jawab untuk pemeliharaan dan dukungan teknik komponen-komponen ini. Akses ke password untuk setiap harus dibatasi pada dua orang – satu primer dan backup. Satu vendor yang memberikan dukungan teknik komponen harus menerapkan prinsip kehati-hatian yang sama (lihat Langkah-12). Jangan pilih opsi pada web browser untuk menyimpan atau mengelola nama dan password pengguna. Tetapkan ketentuan otentikasi untuk akses nirkabel dan rumit.

Langkah-lanjutan

Pertimbangkan penggunaa smart cards atau konten hardware lain untuk akses rumit ke komponen jaringan kritisfirewall,switches, routers. Latih karyawan dalam penggunaan perangkat ini dan rasional penggunaanya, dan berikan tanggung jawab kepada karyawan dalam hal kehilangan atau kerusakan. Cari bantuan teknin (lihat langkah-12) untuk menetaokan pengawasan terhadap intrusi/deteksi untuk memastikan jaringan digunakan sebagaimana mestinya tanpa intervensi dari dalam-atau luar.

Kasus-9 : Pemerasan Cyber menjadi kejadian biasa.

Pemerasan di internet yang suatu saat ditujukan umumnya terhadap individu kaya atau korporasi besar dengan tuntutan pembayaran jumlah besar, sekarang menjadi kejadian biasa bahkan untuk bisnis kecil. Pekerja kantor sekarang melaporkan secara luas menjadi taget pemerasan yang nampaknya menjadikan siapa saja dengan alamta e-mail sebagai sasaran. Tuntutan e-mail yang diminta melalui pembayaran online adalah jumlah uang kecil, biasanya $20-$30. Jika sasaran menolak memenuhi, pengiriman mengancam menyerang sistem komputer perusahaan dan menghapus file sensitive atau memasukan pornografi anak-anak, korban yang merasa tidak curiga, cenderung memilih memenuhi permintaan dari pada menghadapi risiko potensi serangan atau menggangu cyber tidak dilaporkan dan investigasi juga tidak dilakukan.

Langkah-10 : Batasi Akses ke Data Sensitif dan Konfidensial

Biaya : Moderat sampai Tinggi tergantung opsi yang dipilih
Tingkat Keahlian Teknis : Moderat sampai Tinggi
Peserta : Bagian teknik

Mengapa Harus Melakukannya?

e-mail seharusnya hanya dilihat oleh mereka kepada siapa e-mail dikirim. File data seyogyanya hanya diakses oleh individu yang memiliki ijin khusus. Karena anda tidak dapat mempercayai siapapun di dunia untuk berperilaku sesuai norma/aturan, mekanisme control diperlukan untuk menetapkan restriksi. Jika data disimpan dalam file, folder dan basis data dalam jaringan, anda dapat

mengendalikan siapa dapat melihat dan menggunakannya dengan suatu *Access Control List,* atau ACL. ACL menetapkan siapa dapat melakukan tindakan pada suatu file atau folder seperti membaca dan menulis.

Ketika akses ke informasi tidak dapat dikendalikan secara ketat, seperti e-mail atau transaksi katu kredit melalui internet, informasi ini dapat disembunyikan dengan proses matematis yang disebut enkripsi. Enkripsi merubah informasi dari satu bentuk (teks yang bisa dibaca) ke bentuk lain (teks terenkripsi atau teracak). Teks terenkripsi ke setiap informasi dalam jaringan. Ketika siapapun dapat mengakses jaringan anda, mereka dapat melihat setiap komunikasi yang lewat diantara perangkat dalam jaringan anda dan melihat dan memodifikasi atau merusak isinya. Penyedap akan memulai program untuk mencari nomor kartu kredit, social security, dan informasi financial untuk maksud jahat dalam jaringan komunikasi anda. Mereka akan mencari password ke basis data, aplikasi dan jaringan lain untuk memperluas kapabilitas aksesnya.

Pap yang terjadi tanpa Keamanan Data yang Baik?

Keamanan jaringan yang baik (lihat Langkah-9) tidak cukup untuk menjamin perlindungan data. Banyak pihak seperti karyawan tetap, paruh-waktu, dan temporer, juga kontraktor dan vendor, akan memiliki akses formal ke jaringan anda tetapi tidak akses tanpa restriksi ke setiap informasi dalam jaringan. Ketika siapapun dapat mengakses jaringan anda, mereka dapat melihat setiap komunikasi yang lewat diantara perangkat dalam jaringan anda dan melihat dan memodifikasi atau merusak isinya. Penyadap akan memulai program untuk mencari nomor katu kredit, social security, dan informasi financial untuk maksud jahat dalam jaringan komunikasi anda. Mereka akan mencari password ke basis data, aplikasi dan jaringan untuk memperluas kapabilitasi aksesnya.

Langkah Awal

Latih karyawan untuk berhati-hati dalam berbagai informasi sensitive dan konfidensial secara elektronik. Jangan gunakan informasi riel untuk mencoba proses baru. Jangan gunakan komputer publik atau internet Café untuk mengakses layanan financial online atau melakukan transaksi finansiel. Jangan

berikan informasi personal, fiansial atau kartu kredit ke situs web yang tidak dikenal atau dicurigai.

Langkah-lanjutan

Pastikan bahwa browser anda mendukung enkripsi yang kuat (paling tidak 128-bit). Dapatkan bantuan teknik (lihat Langkah-12) untuk menggunakan enkripsi otomatis, jika mungkin, untuk semua komunikasi elektronik keluar jaringan anda, dan beritahu pengirim ketika informasi tidak dapat dikirik dengan enkripsi. Dapatkan bantuan teknik untuk menetapkan cara mengenkrip informasi sensitive dan konfidensial yang disimpan dan dapat diakses dalam jaringan.

Matikan fitur Caching untuk browser sehingga informasi sensitive dan konfidensial tidak disimpan dalam lokasi temporer yang tidak terproteksi. Tetapkan ACL untuk akses ke semua file, folder, dan basis data bersama untuk memastikan bahwa akses hanya tersedia untuk mereka yang memilki ijin. Ini harus dipelihara untuk waktu tertentu karena perubahan staf. Lebih jauh batasi siapa yang dapat meng-update dan menghapus data dan file untuk proteksi maksimal

Kasus-10 : Karyawan Credit Inoin Memanfaatkan informasi Pelanggan untuk keuntungan Pribadi

Departemen Kehakiman AS menuntut seorang wanita yang bekerja disebuah Credit Union. Wanita tersebut menggunakan kmputer Credit Union untuk mendapat informasi account termasuk nama, nomor social security, SIM dan alamt untuk membuka account atas nama orang lain dan melakukan ubauthorized charges. Beberapa rekening kartu kredit dibuka di internet. Setelah membuka rekening palsu, wanita tersebut melakukan berbagai pembelian sampai jumlagh di atas $50,000.

Langkah-11 : Tetapkan dan ikuti suatu Rencana Manajemen Risiko Keamanan Finansial ; Pelihara Jaminan Asuransi yang memadai

Biaya **:** Moderat-metodologi manajemen risiko gratis

Tingkat Keahlian Teknik : Rendah sampai Moderat
Peserta : wakil dari semua level organisasi dan bagian teknik

Mengapa Harus Melakukannya?

Agar efektif, keamanan harus diterapkan secara konsisten di seluruh strata organisasi. Misalnya, penggunaan control teknologi yang sangat ketat tanpa diikuti suatu kebujakan keamanan organisasi sama saja dengan tidak ada perlindungan keamanan.
Cara terbaik untuk validasi keamanan anda adalah memalui aplikasi dari suatu metologo manajemen risiko keamanan. Dalam suatu sekuens kegiatan terstruktur, pserta dari semua level organisasi bekerja bersama untuk menyususn suatu rencana yang logis untuk kebutuhan organisasi berdasarkan penggunaan teknolog-nya. Agar komprehensif rencana proses ini harus mempertimbangkan hal-hal berikut:

1. *Security awareness* dan pelatihan untuk semua pengguna teknologi
2. Kebijakan keamanan organisasi dan regulasi
3. Manajemen keamanan kolaboratif (partner, pihak ketiga dan kontraktor)
4. Rencana kontingensi dan pemulihan bencana
5. Keamanan fisik
6. Keamanan jaringan dan data

Dalam Kesibukan kegiatan sehari-hari sangat mudah untuk melupakan kebutuhan seperti pelatihan keamanan karyawan, rencana kontigensi, dan pemulihan dari bencana. Anda mungkin tidak menyadari tigkat letergantungan organisasi yang telah anda bagun terhadap teknologi dan potensi dampak yang disebabkan jika satu atau lebih komponen gagal berfungsi. Dengan membangun atu rencana manajemen risiko keamanan, ketergantungan ini akan diperiksa untuk mengurangi potensi dampak kebocoran atau kegagaln teknologi.

Apa yang terjadi tanpa manajemn risiko keamanan?
Tanpa suatu rencana, anda harus bereaksi ketika terjado kebocoranatau kegagalan teknologi. Pilihan respons anda akan terbatas oelh apa yang anda dapat temukan ketika masalah terjadi. Juga, anda tidak akan berada pada kondisis

baik untuk menegoisasikan biaya bantuan teknik atau tingkat kepakaran yang diberikan. Kegagalan akan berjalan lebih lama dari pada seharusnya saat anda terburu-buru mencoba melakukan apa yang harus dilakukan untuk mengatasi masalah tersebut.

Langkah Awal

Tinjau rencana pemulihan bencana dan kontigensi. Identifikasi dampak terhadap bisnis anda sekiranya anda mengalami kegagalan pasokan listrik, banjir atau angin rebut berkepanjangan.

Langkah-Lanjutan

Terapkan desain metodologi manajemn risiko keamanan untuk bisnis keil dan menengah (UKM), untuk mengidentifikasi aset teknologi penting, dan kembangkan satu rencana keamanan untuk organisasi anda. Dalam bagian metodologi ini anda akan bandingkan praktek keamanan yang ada dengan standar praktek terbaik untuk mengidentifikasi area kerawanan organisasi dan mekanisme untuk mengatasi kekurangan dalam prosedur yang ada.

Dapatkan bantuan teknik (lihat Langkah-12) untuk melakukan asesmen kerawanan dalam lingkungan teknologi anda guna membantu mengidentifikasi kerawanan yang menjadi risiko utama terhadap aset teknologi penting anda dan mekanisme untuk mengurangi potensi dampaknya.

Kasus-11 : Usaha Ritel On-Line salah menafsirkan Jaminan Asuransi, Pailit Karena Serangan Cyber.

Akibat satu seri serangan komputer, satu usaha ritel online yang sebelumnya bernilai dari $1 juta menjadi pailit. Kehancuran terjadi ketika penyerang mengirim spam kepada pelangganya menuduh bahwa usaha ritel tersebut adalah samara untuk *pedophiles* (isterinya mengelola satu *day care centre).* Kerugian langsung, *denial of service,* penggantian data, kehilangan customer dan biaya PR telah melumpuhkannya. Karena ini adalah pekerjaan orang dalam tidak ada langkah-langkah teknis yang mungkin melindunginy, tetapi manajemen risiko yang memadai termasuk asuransi mungkin menolongnya. Celakanya, pimpinan usaha

ritel telah salah mengerti karena dampak risiko serangan cyber tidak termasuk dalam polisi standar property dan kerugiannya.

Polis standar asuransi tidak mengcover risiko serangan cyber. “bisnis saya hancur, demikian pula bisnis isteri saya, saya hanya berharap masih bisa mempertahankan rumah kami,”. Kata mantan pemilik usaha ritel dengan sedih. Asuransi cyber, yang sekarang tersedia, mungkin menyelamatkan usahanya. Tentu saja, mengambil polis *cyber* terpisah akan menambah pengeluaran operasinya, tetapi mungkin akan menyelamatkan usahanya dari konsekuensi fianansial karena serangan cyber.

Langkah-12 : Dapatkan ekspertis Teknis dan Bantuan Luar dimana perlu

Biaya **:** Rendah sampai Tinggi tergantung layanan yang dibituhkan
Tingkat Keahliak Teknik : Medium sampai tinggi
Peserta **:** Manajemen Perusahaan dan Bagian Teknik

Dapatkan Bantuan yang Tepat
Karena anda punya bisnis untuk dijalankan dan keamanan teknologi bukanlah sesuatu yang boleh dibarkan menyita waktu anda, bantuan teknik yang tepat dapat menjadi suatu aset yang berharga.karyawan, teman, dan keluarga dengan pengetahuan teknis dapat membantu memulainya, tetapi anda membutuhkan seseorang dengan keahlian dan pengalaman keamanan guna menyatukan kegiatan individual karyawan bersama menjadi suatu mekanisme fungsi perlindungan keamanan bagi organisasi anda. Ini pun tidak memberukan jamin perlindungan, karena potensi serangan baru terjadi setiap halnta tool software dan komponen hardware, teknologi keamanan tidak dapat dipelajari melalui “trial and error”. Keamanan bukanlah sesuatu yang statis dan harus sering ditinjau kembali untuk mengidentifikasi ketika perubahan organisasi dan ancaman baru memrlukan penyesuaian pada beberapa atau semua mekanisme perlindungan,

Kehati-hatian harus diperhatikan dalam memilih siapa akan megelola keamanan teknologi organisasi anda. Boleh percaya tetapi [perlu diverivikasi. Mereka yang

dipercaya dengan keamanan akan sangat memahami kelemahan teknologi anda dan bagaimana memanfatka-nya. Pastikan mereka dapat menjelaskan apa yang mereka harus mampu menunjukan bagaimana langkah-langkah itu bekerja menahan serangan untuk anda, mengenali intrusi, dan memulihkan kembali sebagaimana diperlukan.

Apa yang terjadi ekspertis Teknis yang baik

Komponen perangkat keras dan lunak didesain untuk mudah ipasang dan digunakan. Berbagai macam kapabilitas pemakainan bersama informasi tersedia tetapi tidak harus digunakan tanpa petimbangan matang. Waktu dan upaya ekstra diperlukan untuk mengimplementasikan keamanan, tetapi tanpa keamanan jaringan anda retan srangan dan informasi anda dapat diambil atau dirusak menyadari adanya indikasi untuk itu.

Penyerang internet selain mencoba menerobos semua jenis komponen untuk tujuan yang tidak diketahui dan mencuri data, mencari data untuk memperoleh data pribadi dan finansiel, sedang lainnya seperti pesaing anda, karyawan atau mantan karyawan, dan anggota keluarga mungkin ingin mengetahui informasi bisnis, karyawan , dan pelanggan anda. Apapun motifnya, apa sekedar ingin tahu atau ada maksud tidak baik, dampaknya terhadap organisasi adalah hilangnya reputasi bisnis, potensi kerugian kepada pelanggan, denda atau penalty, dan hilangnya waktu untukk menjelaskan bagaimana ini bisa terjadi.

Langkah Awal

Tanyakan pada pihak yang menanggani dukungan teknologi anda bagaimana mereka manjalankan peraktek keamanan dalam buku pedoman ini dan jika mereka perlu bantuan untuk itu. Ketika mempertimbangkan bantuan luar, avaluasi hal-hal berikut :

1. Tinjau pengalaman kerja yang lalu
2. Cari tahu dari beberapa pelanggan lama dan minta referensi dari pelanggan yang sekarang
3. Tanyakan berapa lama perusahaan telah melakukan bisnis

4. Tanyakan siapa, khususnya, akan ditugaskan melakukan pekerjaan nada dan kualifikasi mereka serta sertifikasinya
5. Tanyakan bagaimana mereka akan memebrikan dukungan, apa yang dilakukan di tempat dan apa di luar tempat kerja
6. Tanyakan bagaimana akses diluar tempat kerja dikendalikan

Pastikan anda membuat pengaturan untuk semua praktek keamanan yang dideskripsi dalam pedoman ini. Jika staf internal yang menangani pekerjaan teknis dengan bantuan seorang konsultan, pastikan semua tahu apa yang harus mereka lakukan dan bagaimana meraka akan bekerja bersama. Pastikan anda telah mempertimbangkan persyaratan kinerja minimal, mekanisme pengawasan, dan proses terminasi sebelum menetapkan dukungan keamanan teknis.

Langkah-lanjutan

Malalui organisasiseperti dagangan, asosiasi manufaktur nasional, Federasi Pengusaha Independen, dan grup profesi dan konferensi lain, Tanya pendekatan mereka terhadap keamanan dan apakah mereka merasa telah berhasil. Tentukan evaluasi periodic layanan keamanan anda, baik ditangani internal atau eksternal (minimal sekali setahun dan lebih baik setiap tiga bulan sekali) untuk menentukan apa dukungan yang sekarang cukup dan apa diperlukan peningkatan.

Kasus-12 : Usaha Riset Modal Ventura dan Firma Hukum mencoba bertahan tanpa Bantuan Teknis-Menyesali Keputusan

Perusahaan riset modal ventura dengan tiga orang partner, menemukan kenyataan bagaimana ketergantungan bisnis mereka pada internet ketika e-mail mereka gagal karena virus, sesaat sebelum dua orang partner akan melakukan perjalanan bisnis cukup lama. Meski mereka menerima lebih 600 e-mail seminggu dan menggunakan web sebagai satu-satunya sarana promosi, mereka merasa tidak mampu memperkerjakan eksper teknis *full time.* Mereka membatalkan perjalanan bisnis karena kuatir kehilangan pelanggan. Setelah tiga hari sibuk mencari bantuan, pada akhirnya mereka menemukan seorang pakar untuk membahas masalah mereka.

Sebuah Firma Hukum dengan Kurang lebih 20 buah komputer kehilangan administrator jaringan dan tidak berhasil menggantinya selam 6 bulan. Ketika mereka akhirnya menemukan konsultan, mereka menemukan berbagai kerawanan. Selain itu, update tidak dilakukan pada server, software antivirus tidak diupdate dan lisensi telah berakhir. Setelah konsultan teknis menyampaikan laporan analisa, sebelum mereka mulai perbaikan situasi, firma tersebut diserang virus. Banyak PC terserang dan ratusan file rusak.