

# **Pedoman Praktis Keamanan Informasi Untuk Organisasi Skala Kecil Dan Menengah**

**Studi Kasus Serangan Dan 12  
Rekomendasi Langkah Pengamanan**



**Direktorat Sistem Informasi Perangkat  
Lunak Dan Konten  
Direktorat Jenderal Aplikasi Telematika  
Departemen Komunikasi Dan Informatika  
2006**

# Daftar Isi

- A. Pendahuluan – Usaha Kecil dan Menengah rentan terhadap serangan *cyber*
  - 1. Saya sangat sibuk; Haruskah saya membaca ini?
  - 2. Contoh Nyata Sehari-hari; Ini Dapat Terjadi pada Anda!
  - 3. Apakah Publikasi ini Cocok untuk Bisnis Saya?
  - 4. Mengapa Seseorang akan Menyerang Saya?
  - 5. OK, Mungkin Saya harus lakukan sesuatu, tetapi berapa besar biayanya?
  - 6. Bagaimana bisa saya tetap updated tentang apa yang saya lakukan untuk mengamankan bisnis saya?
  
- B. 12 – Langkah Program Keamanan dan Studi Kasus
  - 1. Langkah–1 : Gunakan Password yang kuat dan Rubah secara reguler  
  
Kasus 1 : Kontraktor dirugikan mantan karyawan menggunakan Akses EMail lama
  
  - 2. Langkah–2 : Waspadai *attachment*

## Email dan *Download* Modul Internet

Kasus 2 : Satu di antara tiga UKM diserang *Worm MyDoom*

3. Langkah-3 : Pasang, Pelihara dan Aplikasikan Program Anti-Virus

Kasus 3 : Konsultan gagal meng-update *Software*, terinfeksi virus dan kehilangan pelanggan

4. Langkah-4 : Pasang dan Gunakan *Firewall*

Kasus 4 : Koneksi Internet *Wireless* hotel rentan pencurian data

5. Langkah-5 : Hapus *Software* dan *Account* yang tidak digunakan; Sterilkan dulu semua peralatan yang diganti

Kasus 5 : UKM Telekomunikasi kehilangan client ketika kebocoran keamanan diketahui Calon Pelanggan

6. Langkah-6 : Terapkan Kontrol Akses Fisik pada semua Peralatan Komputer

Kasus 6 : UKM Akuntansi menyadari pentingnya mengintegrasikan keamanan Fisik dan *Cyber*

7. Langkah-7 : Buat *Backup* untuk File, Folder, dan Software Penting

Kasus 7 : UKM Manufaktur Kehilangan Kontrak Pemerintah karena Software "Time Bomb"

8. Langkah-8 : Rawat dan Lakukan

## *Update Software Mutakhir*

Kasus 8 : Usaha Restoran Mengalami Masalah Logistik karena serangan Virus

9. Langkah-9 : Jaga Keamanan Jaringan dengan Kontrol Akses

Kasus 9 : Pemerasan Cyber Merambah Usaha Bisnis Kecil

10. Langkah-10 : Batasi Akses ke Data Sensitif dan Konfidensial

Kasus 10 : Usaha Perkreditan terkena penipuan Cyber

11. Langkah-11 : Bangun – Terapkan Rencana Manajemen Risiko Keamanan Finansial dan Pelihara Jaminan Asuransi yang memadai

Kasus 11 : UKM Ritel On-Line Salah Mengerti Jaminan Asuransi, Pailit akibat Serangan Cyber

12. Langkah-12 : Cari Bantuan dan Ekspertis Teknis Ketika dibutuhkan

Kasus 12 : UKM Modal Ventura dan Konsultan Hukum Menyesal Berusaha Tanpa Bantuan Ekspertis Teknik

## 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.

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

Penyebaran serangan anonim oleh virus populer seperti "*Code Red*," "*Blaster*," dan "*So Big*" telah meningkatkan publisitas karena dampak negatif atas semua jenis usaha telah meningkat. Perkiraan asuransi menunjukkan 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

di mana 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 reguler. Bagaimana buruk dampak kehilangan bisnis komputer anda terhadap kemampuan anda berusaha secara normal kembali?

Berapa besar biaya untuk memperbaikinya?

Berapa banyak data yang hilang dan tidak tergantikan?

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

Dapatkah anda bangkit mengatasi kesulitan dan kemacetan usaha ini?

## **Contoh Nyata Sehari-hari – Ini Dapat Terjadi pada Anda**

Akibat satu seri serangan komputer, sebuah perusahaan yang sebelumnya bernilai \$ 1 juta, sekarang harus menjual daftar pelanggannya. “Bisnis saya pailit. Bisnis isteri saya juga bangkrut. Sekarang saya hanya berharap masih bisa mempertahankan rumah saya,” kata mantan pemilik perusahaan dengan sedih, seperti dirujuk dalam Computer 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 kenyataannya beberapa perusahaan berhasil bertahan dengan baik. Namun, ini bukanlah kasus hipotetikal. Mereka adalah kejadian nyata UKM yang dilaporkan oleh media, ditayangkan 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 limo, perusahaan angkutan dan sekelompok profesional dan konsultan termasuk firma hukum, akuntansi, dan modal ventura.

Penting untuk memahami bahwa bukan besar/kecilnya usaha atau jenis bisnis, yang menjamin melindungi anda dari serangan *cyber*. Jika anda menggunakan Internet, 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 Bisnis saya?**

Satu analisis bahwa UKM menjadi korban serangan *cyber* dalam skala lebih luas dari pada perusahaan besar adalah bahwa banyak perusahaan besar, dengan skala sumber daya ekonomi yang lebih baik, melakukan upaya sistematis 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 dimaksudkan untuk para manajer 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 Praktis 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 karyawan dan aset tahunan bukanlah kriteria 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 jaring komputer.

Pedoman Praktis untuk Pimpinan Organisasi mungkin berlebihan untuk perusahaan seperti ini. Sebaliknya, sebuah bank kecil, dengan karyawan lebih sedikit dan aset tahunan lebih kecil dari pada perusahaan konstruksi hipotetis di atas, pasti lebih membutuhkan Pedoman Praktis untuk Pimpinan Organisasi, baik karena kebutuhan atau dalam kaitan dengan Pedoman Praktis untuk UKM ini, karena status legal yang kompleks dan lingkungan regulatori terkait dengan industri 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 proteksi sebagai basis melancarkan serangan. Menggunakan komputer tanpa proteksi *firewalls*, *anti-virus software*, dan pelatihan pengguna bukan saja mempengaruhi bisnis anda, tetapi juga mempengaruhi banyak bisnis lain karena virus menyebar di seluruh Internet.

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

Pedoman ini memberi peta jalan menuju keamanan internet secara sederhana 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 pada reaktif.

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

Pada Desember 2003, Departemen Keamanan Dalam Negeri AS berkoordinasi dengan sektor industri menyelenggarakan National Cyber Security Summit yang pertama. Pada kesempatan ini Internet Security Alliance (ISAlliance) diminta untuk menyusun publikasi ini, *A Common Sense Guide to Cyber Security*, satu publikasi *best practices* yang dimaksudkan 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 Manufacturers, 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 mencoba bukan 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 realistis kita mengerti bahwa keamanan berlangsung bertahap, sasaran dari publikasi ini adalah untuk membawa anda melalui semua tahapan. Adalah demi kepentingan bisnis, anda harus mengikutinya secara keseluruhan.

## **Bagaimana Saya Bisa Tetap updated, 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 tinjauan 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 Reguler**

**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 elektronik. Password yang lebih sulit ditebak akan mencegah berbagai jenis *intruder*. UKM sering melakukan pergantian SDM dengan frekuensi yang lebih tinggi, yang justru lebih membutuhkan perubahan password secara reguler. Karena anda tidak tahu bahwa suatu password telah bocor, rubahlah paling tidak setiap 6–bulan sekali dan jika 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 unik.

Dengan tidak menggunakan ulang password lama, kebocoran di satu area tidak akan membuka akses ke area lain. Jangan pernah menulis password pada secarik kertas atau memberitahukan kepada siapapun. Tetapi jika anda perlu menulisnya, simpan kertas itu di tempat yang aman seperti filing cabinet yang

terkunci (tidak di bawah keyboard anda di mana seseorang mungkin akan menemukannya). Setiap pengguna sistem komputer harus memiliki *account* yang unik dan bertanggungjawab dalam memegang password-nya. Ini juga merupakan cara mengkaitkan aksi di jaringan kepada individual tertentu.

### **Password yang Lemah Memberi Rasa Aman Palsu**

Tanpa membatasi akses, semua isi jaringan dapat dilihat, dirubah dan dirusak siapa saja melalui akses jaringan. Jika jaringan terkoneksi ke Internet (sedikit yang tidak, saat ini) informasi anda mungkin bisa diakses dari manapun di dunia. Bahkan dengan password, perlindungan sangat terbatas. *Intruder* 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” password-nya.

Jika mereka tahu sesuatu tentang anda, seperti nama isteri anda, jenis mobil yang anda pakai, 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 menggunakan pola/*pattern* sehingga anda dapat mengingatnya ketika membutuhkannya tanpa harus menuliskannya di atas kertas.

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

## **Langkah-lanjutan**

Bangun lingkungan elektronik yang mempersyaratkan password yang kuat dengan mengharuskan panjang dan struktur password yang kompleks. Terapkan prosedur perubahan passwords secara otomatis untuk mengendalikan kebijakan penggantian password.

**Kasus 1 : Mantan Karyawan menggunakan Akses Email lama guna memata-matai untuk memperoleh keuntungan kompetitif**

Seseorang dari California mengaku bersalah mengakses secara ilegal 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 meneruskannya ke perusahaan baru tempatnya bekerja. Perusahaan lama menanggung kerugian ribuan dollar sebelum akhirnya FBI menghentikan aktivitas ilegalnya.

## **Langkah-2 : Waspada *Attachment* E-mail dan *Download* Modul Internet**

**Biaya** : Minimal – Tidak ada investasi tambahan

**Tingkat Keahlian Teknis** : Rendah sampai medium

**Peserta** : Siapa saja yang menggunakan fasilitas elektronik

### **Mengapa saya harus berhati-hati?**

Satu cara populer mengirim virus komputer adalah dengan menyertakannya dalam satu *attachment* dari suatu e-mail atau materi yang di *download* dari suatu situs web. Belakangan, penyerang semakin ahli mendapatkan buku alamat dan menyertakan virus dalam *attachment* yang nampak datang dari orang yang anda kenal. Perusahaan harus memiliki kebijakan yang ketat tentang apa yang boleh atau tidak boleh di-*download* atau dibuka dalam sistem mereka.

Berbagi informasi via e-mail dan *attachment* memungkinkan kita mengirim laporan, salinan file, spreadsheets, foto, cartoon, musik dsb. Anda meng-update 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 mengecek komputer anda guna memastikan bahwa anda memiliki tool perangkat lunak yang dibutuhkan untuk mengakses konten, dan jika tidak ada, mereka akan secara otomatis melakukan

instalasi untuk anda. Semuanya serba cepat, mudah dan menghindarkan anda dari banyak masalah teknologi yang terlalu rumit.

Seseorang yang menulis suatu program dapat mendistribusikannya di Internet melalui web atau mengirim salinannya sebagai e-mail *attachment*. Anda sangat tergantung pada penulis dari program yang berjalan di komputer anda. Fungsi apa saja yang anda dapat lakukan di komputer anda, program ini juga dapat lakukan. Jika anda menghapus file, mengirim e-mail, atau menambah dan mengurangi program, program yang anda baru pasang juga dapat melakukannya. Seorang *intruder* dapat melakukan hal-hal ini, tanpa 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, dan *download* modul adalah jalan masuk untuk software berbahaya. Dengan membuka satu *attachment* e-mail atau menerima/memasang opsi *download*, program di-copy 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. Jika komputer anda

terserang (*compromised*) setiap orang dalam buku alamat akan menerima e-mail dari anda dengan *attachment* 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 dimasukkan ke komputer anda untuk men-trasir situs web yang anda gunakan dan laporan *account* akses web. Software perekam untuk menyadap, menyimpan dan mengirim sekuen tombol keyboard untuk *account* dan password juga dapat dipasang pada mesin anda.

### **Langkah Awal**

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

1. Jangan gunakan fungsi “preview” untuk konten e-mail.
2. Jangan buka *attachment* yang program anti-virus kenali sebagai berbahaya (lihat Langkah-3)
3. Jangan buka e-mail (hapus saja) dari seseorang yang tidak dikenal, khususnya jika baris subyeknya berisi :
  - Kosong atau berisi huruf dan angka yang tidak bermakna.
  - Memberi tahu anda telah

memenangkan kontes yang anda tidak pernah ikuti atau uang yang anda harus ambil.

- Mendeskripsikan detail produk yang mungkin anda sukai.
- Memberitahu anda tentang masalah dengan instruksi pemasangan software di mesin anda.
- Memberitahu 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 *browser* anda untuk mengingatkan anda terhadap *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 anda tidak pernah *subscribe* karena ini hanya akan memberitahu penyerang bahwa 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 fitur-fiturnya 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-mail pada awal Pebruari 2004. *Worm* datang dengan camouflase *attachment* e-mail, yang, jika dibuka, dapat membuat suatu *backdoor* yang akan membuka akses ilegal ke dalam suatu komputer, yang mungkin dimanfaatkan untuk berbagai tujuan tidak baik di waktu mendatang.

Riset menunjukkan hampir 1 dari 3 UKM telah menjadi korban *Mydoom* dibanding 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. Kerawanan terdapat pada setiap 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, anda perlu periksa adanya virus. Program anti-virus (AV) melihat isi dari setiap file, mencari karakter spesifik yang memiliki profil atau pattern—disebut *virus signature*—yang dikenal berbahaya. Untuk setiap file yang memiliki kesamaan dengan sebuah *signature*, satu program AV memberi

beberapa opsi, seperti menghapus pattern penyerang atau menghancurkan file atau *attachment* e-mail yang berisi virus. Ketika *vendor* program AV menemukan satu virus baru, mereka meng-update *virus signatures* 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 menggunakan virus sebagai cara untuk mendapat akses. Memasang sebuah program AV dan menjaganya tetap up-to-date, di antaranya 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 atau manual minimal setiap minggu. Perbaharui kapabilitas update otomatis setiap tahunnya seperti diperlukan untuk memelihara file *virus signature* up-to-date pada setiap mesin.

Jangan sekali-kali koneksi ke Internet tanpa mengaktifkan program AV terlebih dahulu. Tanamkan kepada semua pengguna komputer untuk menghapus atau menghancurkan file yang teridentifikasi terinfeksi oleh 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 atau tidak dikenal (lihat Langkah-2) untuk mencegah penyebaran virus baru yang belum dapat di-identifikasi program AV.

### **Langkah lanjutan**

Aktifkan program AV untuk secara otomatis memeriksa asal setiap file pada setiap mesin ketika digunakan (CD, floppy, etc.). Jadualkan pemeriksaan AV periodik semua file secara reguler, sebaiknya setiap minggu, untuk menemukan masalah yang mungkin terlewat pada pemeriksaan lain.

### **Kasus-3 : Konsultan tidak meng-update Software ; Akhirnya terinfeksi dan kehilangan pelanggan**

Seorang konsultan utilitas beroperasi sebagai praktisi tunggal membeli sebuah komputer baru untuk mengelola bisnisnya yang sedang berkembang. Si penjual memberitahu komputernya telah dipasang dengan aplikasi anti-virus. Celakanya, si konsultan tidak

menyadari bahwa dia perlu meng-update proteksi ini secara reguler. Tanpa meng-update program anti-virusnya, sistemnya terinfeksi.

Buku alamatnya dimanfaatkan untuk menyebarkan virus kepada para pelanggan melalui e-mail palsu, membawa akibat beberapa pelanggannya memutuskan hubungan 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 penjaga keamanan di suatu gedung umum. Firewall memeriksa pesan yang datang ke dalam sistem anda dari Internet, juga pesan yang anda kirim keluar. Firewall menentukan jika pesan-pesan ini dapat diteruskan ke tujuan atau harus dihentikan. Firewall “penjaga” dapat sangat mengurangi volume pesan yang tidak dikehendaki dan berbahaya masuk ke dalam jaringan anda, tetapi perlu upaya 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 mengizinkan apapun masuk dan keluar (strategi firewall *deny-all*), komunikasi anda dengan Internet sama sekali terputus. Karena ini bukanlah hal yang dikehendaki oleh perusahaan, diperlukan kerja ekstra untuk ini. Beberapa produk firewall memberi kemudahan untuk memeriksa setiap pesan informasi (*packet*) sehingga anda dapat memutuskan apa yang harus dilakukan dengannya. Jika anda hendak membeli sebuah firewall, cari fitur ini karena sangat bermanfaat. Pada hakekatnya, tidaklah mudah untuk menentukan lalu lintas informasi mana yang dapat diterima dan mana yang tidak. Cari bantuan teknik (lihat Langkah-12) untuk membantu anda mengidentifikasi penggunaan normal untuk organisasi anda dan menetapkan aturan untuk memblokir lalu-lintas jaringan yang lain. Firewalls juga dapat digunakan untuk menerapkan kebijakan penggunaan sistem yang akseptable dengan memblokir akses ke situs web yang tidak dikehendaki 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-mail* 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 (*scrutinize*) setiap komputer yang ada dalam jaringan untuk menemukan kerawanan (lihat Langkah-8) dan menyerang.

## **Langkah Awal**

Pasang satu firewall individual pada setiap mesin dan setup untuk memblokir lalu-lintas semua layanan kecuali yang secara spesifik diperuntukkan pada mesin tersebut (lihat Langkah-5). Tanamkan pada para karyawan anda akan nilai dari firewall sehingga mereka akan ikut membantu memperbaiki aturan, dari pada menon-aktifkannya ketika perubahan aturan diperlukan. Sementara aturan firewall dalam proses perumusan, mungkin terjadi hal-hal seperti *over-blocking*, yang membuat operasi beberapa layanan komputer menjadi sulit.

## Langkah lanjutan

Dapatkan bantuan teknik untuk memasang satu atau lebih firewall untuk jaringan anda sesuai konfigurasi sistem. Rumuskan satu kebijakan keamanan untuk dilaksanakan 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 Wireless Internet membutuhkan Firewall**

“Umumnya hotel menawarkan layanan *secure broadband*, tetapi tidak cukup tahu isu-isu keamanan untuk menyampaikan pertanyaan kepada penyedia layanan,” seorang pakar broadband mengatakan kepada CNN. “Seorang tamu dari perusahaan A dapat masuk ke dalam satu konperensi perusahaan B pesaingnya, yang mencuri informasi korporat berharga dan membiarkan hotel menanggung kemungkinan tuntutan kerugian,” CNN melaporkan.

Banyak laptop memiliki setting *default* yang memungkinkan seseorang berbagi file dengan komputer lain. Kecuali ini ditutup, *hackers* akan dapat dengan mudah masuk

ketika seseorang log-on 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 diganti**

**Biaya :** Minimal – Tidak ada investasi tambahan

**Tingkat Keahlian Teknis :** Rendah sampai medium

**Peserta :** Bagian Teknik

**Mengapa Harus melakukannya?**

Sistem komputer diciptakan dengan opsi tak terhitung, banyak di antaranya 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 dihapus dari sistem sehingga tidak dapat digunakan oleh penyerang sebagai sarana untuk merusak sistem anda.

Setiap pengguna komputer harus memiliki *account* yang unik yang membatasi akses ke data dan *software* yang mereka gunakan untuk melakukan tugas (lihat Langkah-1).

Ketika mereka meninggalkan pekerjaan atau berganti fungsi, kapabilitas akses perlu dihapus atau disesuaikan untuk memenuhi tugas baru. Standar teknik pengelolaan, 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 digunakan oleh program pada komputer. Siapa saja dapat *re-trieve* informasi ini dengan mengakses disk dengan komputer lain. Untuk peralatan yang diganti dan dirubah peruntukannya, dibuang, diberikan atau dijual, *disk space* harus dihapus (*overwrite*) untuk mencegah bocornya data konfidensial atau sensitif.

### **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 lain, dan korban dapat menuntut anda atas

kerugian mereka.

Kendali terhadap akses sistem komputing perlu dikelola sebagaimana uang tunai karena kehilangan informasi penting dapat sangat berbahaya bagi bisnis seperti halnya uang. Jika *account* yang tidak digunakan tersebut milik mantan karyawan, mereka akan dapat terus mengakses ke bisnis 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* mantan karyawan ketika mereka berhenti. Ketika memecat seseorang, hapus akses komputernya sebelum memberitahu pemecatan mereka dan lakukan pengawasan selama mereka masih di lingkungan perusahaan. Buat kebijakan bahwa software yang tidak diperlukan tidak dipasang pada komputer perusahaan (seperti games, software gratis, musik dsb). Buat suatu prosedur untuk menghapus data pada semua *hard drive* 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 *clutter* 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 berisiko untuk mempercayakan 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-fungsi komputer 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 awal pemasangan, akan mencegah anda dari masalah besar kemudian.

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

Sebuah perusahaan konsultan telekomunikasi dengan 8-10 karyawan berhasil menjalin perjanjian bisnis dengan sebuah konsultan keamanan untuk suatu proyek bersama. Untuk memastikan,

konsultan keamanan mengirim surat ke pimpinan perusahaan melalui e-mail, yang tidak pernah diterima.

Sebaliknya, konsultan tersebut menerima nota kembali bersama e-mail aselinya yang berbunyi “Jangan melakukan bisnis dengan perusahaan ini. Kami adalah aparat pemerintah dari DEA dan FBI. E-mail ini telah dikirim kepada anda secara konfidensial. Jika anda membuka informasi ini kami akan menuntut anda.” Karena konsultan bekerja di bidang keamanan, dia menganggap bahwa 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 dilaksanakan. Akhirnya diketahui bahwa e-mail palsu dikirim oleh mantan karyawan yang membangun sistem e-mail perusahaan telekomunikasi tersebut. Sebelum keluar meninggalkan perusahaan, dia mengatur agar semua e-mail ke pimpinan perusahaan di-*forward* langsung kepadanya. Yang bersangkutan tidak pernah dibawa ke pengadilan.

**Langkah-6 : Bangun Kendali Akses Fisik untuk semua peralatan komputer**

**Biaya** : Minimal

**Tingkat Keahlian Teknis** : Rendah sampai medium

**Peserta** : Siapa saja yang menggunakan fasilitas elektronik

**Mengapa Harus Melakukannya?**

Bagaimanapun bagus passwords (lihat Langkah-1) dan kontrol keamanan pada komputer, laptop, atau PDA, jika seseorang memiliki akses fisik terhadapnya mereka akan dapat menerobos keamanan dan penggunaannya atau merusak apa saja pada peralatan itu. Peralatan elektronik tidak 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 program 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 network drops) adalah aktif di area terbuka seperti kantor yang kosong, ruang konperensi dan area resepsionis, seseorang dapat menyambung suatu peralatan untuk menerobos jaringan.

## **Kehilangan kendali fisik adalah kehilangan keamanan**

Siapa pun dengan akses fisik ke suatu peralatan elektronik, termasuk repairmen, bagian teknik, dan anggota keluarga, dapat menerobos instalasi kontrol 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 kontrol akan memperlambat mereka tetapi tidak akan menghentikannya, serupa dengan proteksi 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 dibawa 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 pelanggaran 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-out* melalui individu yang bertanggungjawab atas kunci. Didiklah karyawan tentang kebijakan dan lakukan pemeriksaan bahwa kebijakan diikuti dengan baik.

## Langkah-lanjutan

Dapatkan bantuan teknik untuk menerapkan autentikasi semua perangkat *portabel* ketika terkoneksi kembali ke jaringan. Kunci ruang kantor kosong dan ruang konperensi di mana sambungan akses jaringan aktif berada ketika tidak digunakan. Tinjau kontrak dukungan teknik dan layanan perbaikan dengan memasukkan jaminan (*liability*) untuk peralatan dan informasi di dalamnya yang diserahkan untuk perbaikan.

### **Kasus-6 : Perusahaan Akuntansi membuat copy Fisik dan Elektronik-Tetapi Bisnis Terancam Kebakaran**

Satu perusahaan akuntansi berkantor di sebuah gedung bersama dengan sebuah perusahaan angkutan kecil. Perusahaan akuntansi dengan baik membuat backup elektronik dari laporan pajak (*tax return*) pelanggannya dan menyimpan copy fisik dalam filing cabinet bersama dokumen-dokumen penting lainnya. Dia juga mengatur dengan perusahaan akuntansi lain untuk menyimpan copy dari masing-masing arsip perusahaan. Celaknya, terjadi kebakaran pada perusahaan angkutan yang memusnahkan baik file elektronik maupun arsip fisiknya. Namun demikian, dia berhasil mempertahankan bisnisnya hanya karena dia juga menyimpan copy arsipnya di tempat lain.

## **Langkah-7 : Buat Backups dari File, Folders dan Software Penting.**

**Biaya :** Moderat sampai mahal (tergantung tingkat otomasi dan kecanggihan peralatan yang dipergunakan)

**Tingkat Keahlian Teknis:** Medium sampai tinggi

**Peserta :** Bagian Teknik dan Pengguna jika harus menangani backup secara individual

### **Mengapa Harus Melakukannya?**

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 mengganti kerugian karena kecelakaan *cyber*. Backup adalah bentuk lain dari asuransi untuk membantu memulihkan bisnis kembali ketika *intruder* menyerang atau bencana seperti kebakaran atau banjir merusak lingkungan dan aset teknologi anda.

Meng-copy file, 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 perubahan 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 portabel apa saja termasuk floppy disk, CD, *ZIP disks*, atau *disk drive* portabel. Teknik *mirroring* dapat dibangun untuk secara kontinyu membuat duplikasi pada waktu yang bersamaan dengan aselinya untuk pemulihan segera. Copy backup harus disimpan di lokasi aman, sebaiknya ke tempat yang berbeda untuk mencegah kehilangan akibat bencana yang sama dengan aselinya. Kontrol fisik terhadap backups adalah sama penting dengan aselinya (lihat Practice 6).

### **Jika Backup tidak tersedia**

Karena tidak ada proteksi 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. Bahkan dengan backup, proses pemulihan tetap menjadi suatu tantangan, tetapi paling tidak ini masih dimungkinkan.

### **Langkah Awal**

Backup semua file secara periodik sesuai skedul yang ditetapkan. Untuk memilih frekuensi backup yang memadai, perlu diingat bahwa perubahan data asli 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 kalendar atau tahun fiskal perlu disimpan beberapa tahun. Secara berkala periksa proses backup dan akurasi dengan memulihkan 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 berbagai media (*copy file server* dan *copy disk portabel*) untuk memberikan sebanyak mungkin fleksibilitas pemulihan. Pastikan bahwa proses otomatisasi terjadi dengan secara periodik memulihkan konten dan memverifikasi akurasi. Periksa polis asuransi untuk memastikan bahwa data dan

sistem informasi serta hak intelektual anda dijamin seperti halnya properti fisik anda.

**Kasus-7 : Sebuah Usaha Manufaktur kecil Kehilangan Kontrak Besar Pemerintah akibat serangan program “Time Bomb”**

Sebuah usaha manufaktur mendapat kontrak beberapa juta dollar untuk membuat divais 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 manufakturing. Ketika manajer 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 pembangkit program yang memungkinkan perusahaan meng-*customize* produk mereka dan dengan demikian menghemat biaya. Akibatnya perusahaan merugi jutaan dollar, dikeluarkan dari posisinya dalam industri, dan akhirnya harus memberhentikan 80 orang pekerjanya. Perusahaan dapat sedikit merasa lega bahwa pada akhirnya pihak yang bertanggungjawab/bersalah ditangkap dan dihukum.

### **Langkah-8 : Lakukan Update Software secara rutin**

**Biaya** : Moderat – Biaya pemeliharaan Software dan biaya staff untuk memasang dan memverifikasi

**Tingkat Keahlian Teknis** : Medium sampai tinggi

**Peserta** : Bagian Teknik

### **Mengapa Harus Melakukannya?**

*Vendor* software secara rutin menyediakan update (juga disebut *patches*) untuk memperbaiki masalah dan meningkatkan fungsionalitas produk mereka. Sebagai tambahan, banyak dari patch ini memperbaiki kerawanan 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 menyebabkan 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 kustomer untuk memberitahu ketika sesuatu yang tidak diharapkan terjadi ketika software dipergunakan. Dengan tidak melakukan *patches*, anda kehilangan layanan perbaikan terhadap masalah yang diketemukan kustomer 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 anti-virus (lihat Langkah-3) dan firewall (lihat

Langkah-4) serta menambah kerawanan 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 kerawanan 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 memanfaatkannya.

### **Langkah Awal**

Ketika anda membeli suatu program, lihat apakah *vendor* memberikan updates. Perhatikan bagaimana *vendor* memberi 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 kerawanan diberikan.

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

## Langkah-lanjutan

Beberapa *vendor* memberikan program yang secara otomatis meng-kontak situs web *vendor* untuk mencari *patches* baru untuk software mereka. Program ini dapat memberitahu anda ketika *patch* sudah ada, dan dapat *download* dan men-setupnya. Anda sesuaikan fitur-fitur program update yang hanya anda perlukan -- misalnya, memberitahu bahwa *patch* baru telah keluar dan memberi anda opsi untuk men-*download* dan memasangnya. Jika anda menemukan kerawanan dan belum ada *patch* tersedia, pertimbangkan menggunakan program lain sampai program asli berhasil diperbaiki.

### **Kasus-8 : Layanan logistik Rumah Makan Terputus, Sistem Reservasi sebuah Penginapan Crashed, karena gagal melakukan Update**

Beberapa rumah makan yang mempercayakan pada e-mail dalam urusan dengan supplier-nya, terputus layanan logistiknya selama 4-hari karena serangan virus. Meskipun telah mencoba *download patches* untuk mengatasi masalahnya, ternyata tidak banyak bermanfaat karena tidak melakukan *patches* untuk masalah 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. Ditemukan

sistem reservasi online-nya terputus untuk beberapa hari, dan karyawan menjadi kurang percaya lagi pada sistem komputernya karena khawatir juga mengalami malfungsi.

### **Langkah-9 : Terapkan Keamanan Jaringan dengan Kontrol Akses**

**Biaya** : Moderat sampai tinggi tergantung pada opsi yang dipilih

**Tingkat Keahlian Teknis** : Moderat sampai tinggi

**Peserta** : Bagian Teknik dan semua pengguna jaringan

### **Mengapa Harus Melakukannya?**

Meski lingkungan teknologi organisasi anda disebut sebagai “Jaringan”, pada kenyataannya ia adalah kumpulan dari komponen yang disusun sedemikian untuk memenuhi kebutuhan teknologi spesifik 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 memanfaatkan komponen dan layanan jaringan. Sebagai tambahan, *remote device* dan portabel harus diminta otentikasinya ke jaringan untuk membatasi siapa dapat melihat dan mengakses layanan jaringan seperti basis data, file dan printer yang dipakai bersama.

Suatu firewall (lihat Langkah-4) merupakan *buffer* antara komponen-komponen jaringan anda dengan lingkungan eksternal. Teknik lain, seperti server *proxy* dan *Network Address Translation* (NAT) memberi proteksi lebih dalam membatasi informasi mana seorang pengguna eksternal dapat tahu tentang komponen-komponen dalam lingkungan jaringan, membuat lebih sulit bagi penyerang menemukan kerawanan. Semakin banyak restriksi akses yang anda dapat pasang menggunakan kapasitas *blocking* dari firewall dan layanan serupa lainnya, semakin mudah untuk membuatnya aman.

### **Pertimbangan Khusus**

Kontrol akses yang baik sangat kritis untuk akses *wireless* karena penggunaan jenis konektivitas ini agak kurang 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 rimut (dial-in) ke jaringan dan tidak menyadarinya, karena banyak vendor memasangnya untuk dapat memberikan kapasitas dukungan rimut. Perangkat pemasaran dan inventori berkomunikasi ke server sentral melalui *wireless* (nirkabel).

Kemampuan untuk mencapai dan menggunakan layanan jaringan anda dari luar (disebut akses rimut) sangat berharga bagi karyawan, suppliers dan kustomer yang

sering bepergian. Akses rimut juga memungkinkan *vendor* teknologi untuk memberikan dukungan layanan jaringan kritis secara cepat tanpa harus mengunjungi tempat anda. Karyawan dapat dan menambahkan perangkat akses rimut (*dial-in*) langsung ke komputer mereka agar mereka dapat bekerja dari luar.

Penggunaan jenis akses rimut 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-peer*) ke dalam jaringan, menerobos banyak mekanisme keamanan tradisional suatu jaringan. Opsi-opsi ini telah berkembang menjadi akses masuk program berbahaya (*malicious software*) dan harus digunakan secara hati-hati.

### **Apa yang terjadi tanpa Keamanan Jaringan yang baik?**

Penyerang terus-menerus membombardir komponen yang dapat diakses dari Internet dengan *queries* untuk mencari kelemahan. Perangkat tanpa proteksi akan dapat diterobos 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 berisiko karena 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 karyawan lain menggunakan peralatan (*tools*) yang tersedia dari Internet jika keamanan jaringan kurang baik. Peralatan ini memungkinkan untuk memata-matai kegiatan pihak lain, melihat informasi diluar bidang tugasnya, menguntit dan mengganggu pihak lain, dan menanamkan konten berbahaya pada komputer lain.

### **Langkah Awal**

Akses ke setiap komponen dari jaringan harus dibatasi 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 firewalls (lihat Langkah-4), *switches*, dan

*routers* harus dibatasi hanya kepada individu yang bertanggung-jawab untuk pemeliharaan dan dukungan teknik komponen-komponen ini. Akses ke password untuk setiap komponen 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 rimut.

### **Langkah-lanjutan**

Pertimbangkan penggunaan *smart cards* atau *token hardware* lain untuk akses rimut ke komponen jaringan kritis, terutama firewall, *switches*, dan *routers*. Latih karyawan dalam penggunaan perangkat ini dan rasional penggunaannya, dan berikan tanggungjawab kepada karyawan dalam hal kehilangan atau kerusakan. Cari bantuan teknik (lihat Langkah–12) untuk menetapkan 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 target pemerasan yang nampaknya menjadikan siapa saja dengan alamat e-mail sebagai sasaran. Tuntutan e-mail yang diminta melalui pembayaran online adalah jumlah uang kecil, biasanya \$20 – \$30 dollar. Jika sasaran menolak memenuhi, pengirim mengancam menyerang sistem komputer perusahaan dan menghapus file sensitif atau memasukkan pornografi anak-anak. Korban yang merasa tidak curiga, cenderung memilih memenuhi permintaan dari pada menghadapi risiko potensi serangan atau menanggung malu. Konsekuensinya, banyak peristiwa pemerasan 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 kontrol 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 kartu 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 nampak tidak bermakna (*illegible*) dan tetap seperti itu untuk orang yang tidak memiliki formula (skema transformasi enkripsi dan

kunci dekripsi) untuk merubah teks terenkripsi kembali menjadi teks yang bisa dibaca. Mekanisme enkripsi harus cukup kompleks atau seseorang dengan peralatan elektronik dapat menebak formula dan membuka enkripsi.

### **Apa 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 kartu kredit, *social security*, dan informasi finansial untuk maksud jahat dalam jaringan komunikasi anda. Mereka akan mencari password ke basis data, aplikasi dan jaringan lain untuk memperluas kapabilitas aksesnya.

## **Langkah Awal**

Latih karyawan untuk berlaku hati-hati dalam berbagi informasi sensitif dan konfidensial secara elektronik. Jangan gunakan informasi riel untuk mencoba proses baru. Jangan gunakan komputer publik atau Internet Café untuk mengakses layanan finansial online atau melakukan transaksi finansial. Jangan berikan informasi personal, finansial, 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 dikirim dengan enkripsi. Dapatkan bantuan teknik untuk menetapkan cara mengenkrip informasi sensitif dan konfidensial yang disimpan dan dapat diakses dalam jaringan.

Matikan fitur *caching* untuk browser sehingga informasi sensitif 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 memiliki 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 Union memanfaatkan Informasi Pelanggan untuk keuntungan Pribadi**

Departemen Kehakiman AS menuntut seorang wanita yang bekerja di sebuah Credit Union. Wanita tersebut menggunakan komputer Credit Union untuk mendapat informasi *account* termasuk nama, nomor *social security*, SIM dan alamat untuk membuka *account* atas nama orang lain dan melakukan *unauthorized charges*. Beberapa rekening kartu kredit dibuka di Internet. Setelah membuka rekening palsu, wanita tersebut melakukan berbagai pembelian sampai jumlah 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 Teknis** : 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 kontrol teknologi yang sangat ketat tanpa diikuti suatu kebijakan keamanan organisasi sama saja dengan tidak ada perlindungan keamanan.

Cara terbaik untuk validasi keamanan anda adalah melalui aplikasi dari suatu metodologi manajemen risiko keamanan. Dalam suatu sekuens kegiatan terstruktur, peserta dari semua level organisasi bekerja bersama untuk menyusun suatu rencana yang logis untuk kebutuhan organisasi berdasarkan penggunaan teknologi-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 kontingensi, dan pemulihan dari bencana. Anda mungkin tidak menyadari tingkat ketergantungan organisasi yang telah anda bangun terhadap teknologi dan potensi

dampak yang disebabkan jika satu atau lebih komponen gagal berfungsi. Dengan membangun satu rencana manajemen risiko keamanan, ketergantungan ini akan diperiksa dan langkah-langkah yang harus diambil dapat diidentifikasi untuk mengurangi potensi dampak kebocoran atau kegagalan teknologi.

### **Apa yang Terjadi Tanpa Manajemen Risiko Keamanan?**

Tanpa suatu rencana, anda harus bereaksi ketika terjadi kebocoran atau kegagalan teknologi. Pilihan respons anda akan terbatas oleh apa yang anda dapat temukan ketika masalah terjadi. Juga, anda tidak akan berada pada kondisi baik untuk menegosiasikan 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 kontingensi. Identifikasi dampak terhadap bisnis anda sekiranya anda mengalami kegagalan pasokan listrik, banjir atau angin ribut berkepanjangan.

### **Langkah-lanjutan**

Terapkan desain metodologi manajemen risiko keamanan untuk bisnis kecil 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 lebih dari \$1 juta menjadi pailit. Kehancuran terjadi ketika penyerang mengirim *spam* kepada pelanggannya menuduh bahwa usaha ritel tersebut adalah samaran untuk *pedophiles* (isterinya mengelola satu *day care center*). Kerugian langsung, *denial of service*, penggantian data, kehilangan kustomer dan biaya PR telah melumpuhkannya. Karena ini adalah pekerjaan orang dalam tidak ada langkah-langkah teknis yang mungkin melindunginya, tetapi manajemen risiko yang memadai termasuk asuransi mungkin menolongnya. Celaknya, pimpinan usaha ritel telah salah mengerti karena dampak risiko serangan *cyber* tidak termasuk dalam polis standar properti dan kerugiannya.

Polis standar asuransi tidak meng-cover 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 finansial karena

serangan *cyber*.

**Langkah-12 : Dapatkan Ekspertis Teknis dan Bantuan Luar dimana perlu**

**Biaya** : Rendah sampai Tinggi tergantung layanan yang dibutuhkan

**Tingkat Keahlian Teknis** : 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 dibiarkan 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. Inipun tidak memberikan jaminan perlindungan, karena potensi serangan baru terjadi setiap hari. Tidak seperti halnya *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 memerlukan penyesuaian pada beberapa atau semua

mekanisme perlindungan

Kehati-hatian harus diperhatikan dalam memilih siapa akan mengelola keamanan teknologi organisasi anda. Boleh percaya tetapi perlu diverifikasi. Mereka yang dipercaya dengan keamanan akan sangat memahami kelemahan teknologi anda dan bagaimana memanfaatkannya. Pastikan mereka dapat menjelaskan apa yang mereka lakukan dan mengapa. Mereka harus mampu memperagakan langkah-langkah yang dilakukan untuk menerapkan ketentuan keamanan dalam buku pedoman ini. Selanjutnya, mereka harus mampu menunjukkan bagaimana langkah-langkah itu bekerja menahan serangan untuk anda, mengenali intrusi, dan memulihkan kembali sebagaimana diperlukan.

### **Apa yang terjadi tanpa Ekspertis Teknis yang baik**

Komponen perangkat keras dan lunak didesain untuk mudah dipasang dan digunakan. Berbagai macam kapabilitas pemakaian bersama informasi tersedia tetapi tidak harus digunakan tanpa pertimbangan matang. Waktu dan upaya ekstra diperlukan untuk mengimplementasikan keamanan, tetapi tanpa keamanan jaringan anda rentan serangan dan informasi anda dapat diambil atau dirusak tanpa anda menyadari adanya indikasi untuk itu.

Penyerang Internet selain mencoba menerobos semua jenis komponen untuk tujuan yang tidak diketahui dan mencuri data, mencari cara 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 penalti, dan hilangnya waktu untuk menjelaskan bagaimana ini bisa terjadi.

### **Langkah Awal**

Tanyakan pada pihak yang menangani dukungan teknologi anda bagaimana mereka menjalankan praktek keamanan dalam buku pedoman ini dan jika mereka perlu bantuan untuk itu. Ketika mempertimbangkan bantuan luar, evaluasi 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 anda dan kualifikasi mereka serta sertifikasinya
5. tanyakan bagaimana mereka akan memberikan dukungan, apa yang dilakukan di tempat kerja, dan apa di luar tempat kerja
6. tanyakan bagaimana akses diluar

tempat kerja dikendalikan

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

## **Langkah-lanjutan**

Melalui organisasi seperti Kamar Dagang, 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 periodik layanan keamanan anda, baik ditangani internal atau eksternal (minimal sekali setahun dan lebih baik setiap tiga bulan) 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 mempekerjakan eksper teknis *full time*. Mereka membatalkan perjalanan bisnis karena khawatir kehilangan pelanggan. Setelah tiga hari sibuk mencari bantuan, pada akhirnya mereka menemukan seorang pakar untuk membahas masalah mereka.

Sebuah Firma Hukum dengan  $\pm$  20 buah komputer kehilangan administrator jaringan dan tidak berhasil menggantinya selama 6 bulan. Ketika mereka akhirnya menemukan konsultan, mereka menemukan berbagai kerawanan. Selain itu, update tidak dilakukan pada server, software anti virus tidak di-update 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.