Pedoman Praktis
Manajemen Keamanan Informasi
Untuk Pimpinan Organisasi

10 Rekomendasi Terbaik
Manajemen Keamanan Informasi

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 JENDERAL APLIKASI TELEMATIKA

Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. Keberadaan TIK membuat hidup kita menjadi lebih mudah dan menyenangkan. Aktifitas yang terkait dengan pekerjaan, pendidikan, hingga hiburan terkait erat dengan pemanfaatan TIK. Menyusun dokumen elektronik, melakukan perhitungan, e-mail, berselancar di internet, chatting merupakan aktivitas sehari-hari yang memanfaatkan TIK. Saya yakin tidak ada satupun organisasi atau perusahaan yang tidak menggunakan peralatan TIK dalam kegiatannya, bahkan bagi sebagian mereka, TIK sudah menjadi bagian utama pelaksanaan kegiatan.

Layaknya dunia nyata, dalam dunia TIK selain hal-hal baik yang diperoleh, ada juga hal-hal buruk yang mengintai, antara lain seperti virus komputer, spam, cracking, sniffing, dan sebagainya. Kita harus menerima kenyataan bahwa ada orang yang bermaksud tidak baik di luar sana. Saya yakin bahwa setiap pengguna komputer pernah mengalami serangan virus, spam, atau bentuk kejahatan TIK lainnya pada satu ketika dalam hidupnya. Siapa yang tidak kenal ‘’brontok’’, worm made Indonesia, yang dapat menginfeksi suatu computer dan menyebar dengan cepat melalui USB Flash Disk dan jaringan. Banyak computer yang terinfeksi dengan parah tidak dapat dipergunakan hingga mereka dibersihkan atau diformat ulang.Dapat dibayangkan beberapa kerugian dari segi waktu, produktivitas kerja, serta biaya yang harus dikeluarkan untuk membersihkan virus tersebut. Karakteristik serangan virus dapat menyebar luas dengan cepat juga dapat mengancam keberlangsungan operasional suatu organisasi atau perusahaan yang menggantungkan segala aktivitasnya pada TIK.

Bagaimana kita mengatasinya? Sejalan dengan perkembangan teknologi, kejahatan dalam dunia TIK juga berkembang sangat cepat. Kita tidak akan mungkin dapat menuntaskan semua potensi serangan kejahatan TIK tersebut sekaligus. Namun demikian ada langkah-langkah reaktif maupun preventif yang

dapat dilaksanakan guna mengatasi permasalahan tersebut diatas.Langkah-langkah tersebut dirangkum dalam sebuah buku **'pedoman praktis tentang manajemen keamanan informasi untuk pimpinan organisasi'.** Saya menyambut baik dan merasa bangga dengan inisiatif penerbitan buku ini, yang diharapkan dapat meningkatkan kesadaran para pimpinan organisasi akan bahaya ancaman virus komputer dan serangan kejahatan TIK lainnya serta kemampuan mereka dalam mengatasi serangan tersebut.

Salam Aptel

Jakarta, Desember 2006

Cahyana Ahmadjayadi

KATA PENGANTAR

Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian penting yang tidak terpisahkan dari aktivitas keseharian instansi pemerintah. Sejalan dengan perkembangan pemanfaatannya, ancaman terhadap aspek keamanan informasi juga turut meningkat. Serangan virus, worm, dan malware dapat melumpuhkan bahkan menghancurkan suatu sistem informasi yang telah dibangun dan dikembangkan dengan susah payah. Selain itu, penyusup dan *''crackers''* sangat aktif mencari celah untuk dapat masuk kedalam suatu sistem informasi dan melakukan berbagai tindak kejahatan *''cyber''*.Kerugian dari segala ancaman serangan terhadap keamanan informasi ini tidak terhitung nilainya, baik dari segi materil maupun moril, apalagi yang menyangkut rahasia Negara.

Keamanan informasi bukan hanya berkaitan dengan aspek teknologi dan aspek sumber daya manusia saja tetapi juga terkait dengan berbagai aspek lain, seperti aspek manajemen termasuk kebijakan organisasi, sistem manajemen dan perilaku manusia.

Instansi pemerintah pengguna sistem informasi wajib menyelenggarakan pengelolaan keamanan informasi yang menyeluruh untuk melindungi informasinya dari berbagai macam ancaman serangan. Mengelola suatu sistem keamanan informasi bukan merupakan pekerjaan mudah, untuk itu depkominfo mengeluarkan suatu panduan praktis yang dapat menjadi acuan dalam pengelolaan keamanan informasi.

'pedoman praktis tentang manajemen keamanan informasi untuk pimpinan organisasi' ini diadopsi dari *common sense guide for senior managers yang diterbitkan oleh internet security alliance.* Pedoman ini direkomendasikan bagi para pimpinan organisasi untuk mengelola resiko keamanan informasi di organisasinya.

Departemen Komunikasi dan Informatika akan terus memperbaiki dan mengembangkan pedoman praktis ini guna memenuhi kebutuhan aspek keamanan informasi dalam menghadapi berbagai ancaman serangan.

Saran dan masukan terhadap pedoman praktis ini sangat diharapkan sehingga dapat membantu untuk menyempurnakan penulisan selanjutnya. Korespondensi ditujukan ke alamat e-mail: ksi_ditsipik@depkominfo.go.id

Semoga bermanfaat!

Jakarta, Desember 2006

Lolly Amalia Abdullah
Direktur
Sistem Informasi, Perangkat Lunak dan Konten

PENDAHULUAN

Dengan semakin meningkatnya pemanfaatan teknologi informasi dalam berbagai bidang maka resiko ancaman terhadap keamanan informasi juga terus meningkat.Dari berbagai sumber indikasi semakin meningkatnya ancaman terhadap keamanan informasi dapat dilihat baik dari jumlah maupun dari tingkat kecanggihannya. Kerugian finansial yang ditimbulkan sangat besar yang terjadi dalam berbagai bentuk seperti hilangnya pendapatan, besarnya biaya perbaikan, hilangnya data dan kepercayaan pelanggan serta bentuk-bentuk kerugian lain. Kenyataan ini mengharuskan pengguna teknologi informasi baik sebagai pribadi maupun institusi harus siap menghadapi ancaman keamanan informasi ini.

Dapat dipahami bahwa baik pribadi maupun institusi seringkali sudah terlalu disibukkan dengan urusan rutinnya sendiri sehingga masalah keamanan informasi belum mendapat perhatian sebagaimana mestinya pada saat ini. Perlu dimengerti bahwa biaya yang dapat ditimbulkan dari kekurangpedulian ini dapat sangat besar. Hal ini mengharuskan diberikannya perhatian yang layak dari semua pihak pada pentingnya keamanan informasi. Keamanan informasi bukan hanya berkaitan dengan teknologi dan pemilihan teknologi mengatasi ancaman tetapi berkaitan juga dengan berbagai aspek lain dalam manajemen termasuk kebijakan organisasi, sistem manajemen, perilaku manusia dan faktor-faktor lain.

Pedoman ini yang mengambil materi utama dari berbagai sumber yang kompenten membahas 10 dimensi dari pengelolaan keamanan informasi seperti kebijakan, proses, sumber daya manusia, dan teknologi yang semuanya penting untuk penerapan suatu proses keamanan yang baik. Dengan adanya 10 dimensi yang berbeda ini diharapkan semua aspek yang berkaitan dengan proses manajemen resiko didalamnya terliput dengan baik. Besarnya pengaruh setiap dimensi tentunya sangat tergantung pada jenis kegiatan institusi dan kompleksitas sistem informasi yang diterapkan. Diharapkan pedoman ini bisa menjadi acuan bagi para pimpinan organisasi dan pihak lain yang langsung terlibat di bidang ini, dalam memahami masalah keamanan informasi dan dalam memberikan dukungan bagi penerapan sistem keamanan informasi pada insitusi

masing-masing.

Dengan berkembangnya teknologi informasi dari waktu ke waktu perlu dilakukan penyesuaian-penyesuaian dalam pengelolaan keamanan informasi, sehingga pedoman ini juga akan memerlukan penyesuaian-penyesuaian dalam pengelolaan keamanan informasi, sehngga pedoman ini juga akan memerlukan penyesuaian-penyesuaian pada masa yang akan datang. Diharapkan pedoman ini bisa menjadi refrensi yang berguna bagi pribadi-pribadi maupun institusi yang mengembangkan dan memerapkan sistem keamanan informasi masing-masing. Tim perumus akan senang sekali menerima koreksi dan saran-saran perbaikan untuk keperluan penyempurnaan di masa mendatang.

PEDOMAN NO. 1

Manajemen umum

Manajer semua organisasi beranggapan bahwa keamanan informasi adalah bagian dari tanggungjawab manajemen dan karyawan.Manajer menetapkan dan membagi tugas dan tanggungjawab keamanan informasi untuk memastikan bahwa cukup sumber daya dialokasikan untuk semua kebutuhan ini.

> *Langkah-langkah manajer mencakup memberi pengarahan, komunikasi tertulis, dan pertemuan dengan staf atas subyek terkait. Manajer menetapkan, memeriksa pelaksanaan dan mengevaluasi secara regular kebijakan keamanan (lihat pedoman no.2)*

Hal-hal yang harus diperhatikan pimpinan, pimpinan organisasi dan dewan pengawas:

- Apakah manajemen senior, termasuk direksi, menetapkan kebijakan keamanan informasi dan internet dan proses audit?
- Apakah keamanan dipandang sebagai suatu kegiatan rutin atau esensiel untuk ketahanan bisnis? Apakah pertimbangan keamanan suatu bagian rutin dari proses bisnis anda?

- Apakah ada ketentuan legal atau regulasi yang harus diikuti baik sebagai komitmen kontrak atau sektor industri di mana anda beroperasi
- Apakah manajer di setiap level organisasi memahami tugas dan tanggungjawab terkait keamanan informasi? Bagaimana anda memverifikasinya? Apa anda mengerti tugas anda?

PEDOMAN NO.2

Kebijakan

Kembangkan, terapkan, tinjau ulang, dan laksanakan kebijakan keamanan yang memenuhi sasaran bisnis.

Rumuskan kebijakan untuk menangani kunci keamanan seperti manajemen risiko keamanan, identifikasi aset kritis, keamanan fisik, manajemen sistem dan jaringan, otentikasi dan otorisasi, akses control, manajemen kerawanan, awareness dan pelatihan, dan privasi.

Pastikan bahwa maksud dari setiap kebijakan tercermin dalam standar, prosedur, pedoman, pelatihan, dan arsitektur keamanan implementasinya.

Hal-hal yang harus diperhatikan pimpinan organisasi dan dewan pengawas?

- Apa kebijakan keamanan organisasi yang paling penting dan untuk memenuhi sasaran bisnis apa kebijakan tersebut?
- Apa peran anda dalam menjamin bahwa kebijakan keamanan diikuti?
- Apa konsekuensi jika kebijakan tersebut tidak diikuti?
- Apa ada konsekuensi hukum jika standar tertentu kehati-hatian tidak diikuti?
- Jika perusahaan anda sebuah perusahaan publik dan melakukan bisnis internet, apakah risiko pendapatan e-commerce dilaporkan dalam SPT tahunan seperti ditentukan UU?

PEDOMAN NO.3

Manajemen risiko

Secara berkala lakukan suatu evaluasi risiko keamanan informasi yang mengidentifikasi aset informasi kritis (diantaranya sistem, jaringan, data), ancaman terhadap aset kritis, kerawanan asset, dan risiko.

Identifikasi dampak ekstrim jika risiko terhadap aset kritis terjadi termasuk finansial, reputasi, posisi pasar, waktu/produktivitas dsb. Perhitungkan dampak finansial semaksimal mungkin.

Susun dan implementasikan satu rencana penanggulangan risiko hasil penanggulangan risiko hasil evaluasi (diupdate jika perlu)

Pastikan bahwa ada peninjauan regular dan manajemen terhadap risiko aset informasi kritis.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

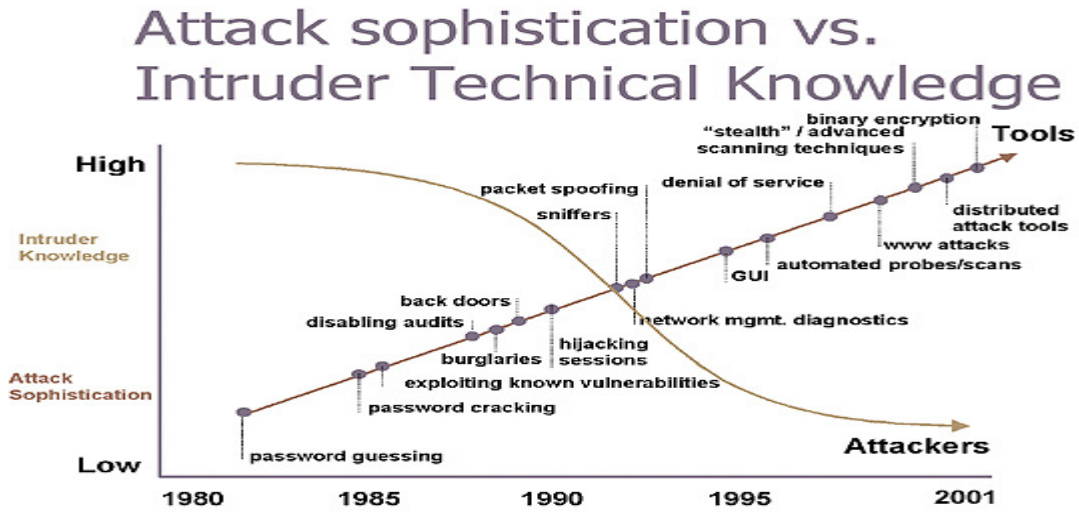
- Bagaimana organisasi anda mengidentifikasi aset informasi kritis dan resiko atas aset tersebut?
- Adakah aset kritis yang menjadi tanggung jawab anda?
- Apakah frekuensi dan skala dari evaluasi risiko anda memadai untuk memperhitungkan ancaman yang ada?
- Apakah risiko terhadap aset kritis dikelola sebaik risiko kunci bisnis lain? Apakah semua aset kritis ditinjau setiap tahun dalam suatu audit eksternal?
- Apa potensi dampak finansial terhadap terjadi serangan atas aset ini?

Jaga keseimbangan biaya investasi keamanan dengan kerugian akibat pelanggaran keamanan untuk menyeimbangkan aspek toleransi perusahaan terhadap risiko.

Data from dr. William M. hancock, Exodus, A cable and wireless service.

Peningkatan dalam kecanggihan perangkat serangan membutuhkan penurunan pengetahuan teknis intruder.

Sumber : CERT coordination center



PEDOMAN NO.4

Arsitektur & desain keamanan

Susun, implementasikan, dan jaga arsitektur keamanan perusahaan (atau situs), bedasarkan kebutuhan sasaran bisnis dan lindungi aset-aset informasi paling kritis.

> *Terapkan pendekatan berlapis (diantaranya, jaringan, host, aplikasi, data) termasuk pedoman yang mengikutinya.*
>
> *Gunakan keberagaman dan solusi redunan (power supplies-catu daya, telekomunikasi, hardware, sistem operasi, aplikasi) untuk sistem dengan resiko atau ketergantungan tinggi.*

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Apakah komponen utama arsitektur keamanan organisasi anda? Apakah proses kesesuaian dan kehati-hatian termasuk review potensi sumber-sumber out-source?
- Apa sasaran bisnis yang harus dipenuhi oleh arsitektur keamanan anda?
- Adakah proses untuk menentukan dampak keamanan mengintegrasikan sistem baru ke arsitektur sistem lama perusahaan anda?
- Aset apa paling perlu perlindungan keamanan dan mengapa? Apa lima fungsi bisnis paling kritis yang tergantung aset ini?
- Jika tidak tahu, kepada siapa anda bertanya?

PEDOMAN NO.5 : isu-isu pengguna

PEDOMAN NO. 5.1

Isu pengguna : akuntabilitas dan pelatihan

Susun peraturan akuntabilitas untuk setiap aksi pengguna, lakukan pelatihan akuntabilitas dan tegaskan pelaksanaannya, seperti tercermin dalam kebijakan dan prosedur organisasi. Pengguna termasuk semua yang memiliki account aktif

sebagai karyawan, partner, pemasok, dan rekanan.

Pengguna harus menganggap keamanan informasi sebagai bagian rutin dari tanggung jawab harian mereka.

Sebelum menerima penugasan, pengguna harus dilatih dalam semua topic kebijakan sepertipemilihan dan proteksi password, ijin akses file, harapan privasi, web browsing aman, dan social enigeneering.

Pengguna harus dilatih tentang implikasi dan sanksi terkait dengan pelanggaran kebijakan termasuk konsekuensi legal.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Kapan terakhir kali anda dan manajer senior lain, termasuk dewan pengawas, mendapat briefing atau mengikuti pelatihan keamanan informasi untuk pengguna sebagaimana diterapkan dalam organisasi anda?
- Apakah fungsi audit koporat anda termasuk kebijakan keamanan dan priview pedoman? Apakah ada proses yang dapat diaudit atas kebijakan pengecualian guna membatasi konsekuensi legal perusahaan jika karyawan menggunakan sistem untuk maksud tidak baik atau illegal?
- Apakah tanggung jawab anda untuk ikut memastikan bahwa pedoman ini diikuti dengan baik?

PEDOMAN NO. 5.2

Isu pengguna: ekspertis yang memadai

Pastikan bahwa ada cukup eksper internal atau jelasnya eksper bantuan untuk semua teknologi yang ada (yaitu sistem operasi host dan jaringan, router, fire-wall, perangkat monitor, dan software aplikasi), termasuk operasi aman dari semua teknologi tersebut.

Hal-hal yang harus diperhatikan pimpinan, manajer senior, dan dewan pengawas?

- siapa yang anda hubungi ketika anda memiliki masalah dengan sistem

operasi, laptop, akses ke data proyek baru, password, aplikasi keamanan, aplikasi khusus yang dirancang dan dibangun sendiri?

- Siapa yang anda hubungi ketika firewall korporat anda memblokir akses ke suatu layanan yang anda perlukan?

PEDOMAN NO.6 : Manajemen sistem & jaringan

PEDOMAN NO. 6.1

Manajemen sistem &jaringan : kontrol akses

Buat satu rangkaian kontrol keamanan untuk melindungi aset yang ada dalam sistem dan jaringan.

Gunakan kontrol akses untuk jaringan, sistem, file dan level aplikasi dimana perlu.

Gunakan enkripsi data dan teknologi Virtual Private Network (VPN) di mana perlu.

Gunakan aplikasi keamanan perimeter dan internal (termasuk firewalls) yang menerapkan kebijakan keamanan.

Gunakan media penyimpanan portable untuk data kritis agar dapat dinamakan secara fisik.

Tetapkan satu prosedur penghapusan sistem untuk menghapus semua data dalam disk dan memori yang akan dimusnahkan/diganti.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Bagaimana anda memastikan bahwa setiap karyawan hanya memiliki akses ke file, direktori, dan aplikasi terkait dengan tanggung jawab tugasnya dan apa yang diperlukan? Beberapa seiring ijin dievaluasi untuk kelaikan dan akurasi?
- Bagaimana anda menciptakan pasangan kunci publik/privat untuk meng-

ekripsi informasi sensitif?

- Bagaimana anda berbagi kunci publik anda dengan yang lain dan bagaimana yang lain berbagi kunci mereka dengan anda?

PEDOMAN NO. 6.2

Manajemen sistem &jaringan : intregitas perangkat lunak

Verifikasi secara reguler integritas dari perangkat lunak yang dipasang.

Periksa secara berkala dan hapus semua virus, worms, Trojan horse, malicious software lain dan software tanpa otoritasi.

Periksa dan bandingkan secara leguler semua file dan direktori dengan metoda ''checksum kriptografis'' dengan perbandingan dasar yang disimpan dan dipelihara secara aman.

Hal-hal yang harus diperhatikan pimpinan, manajer senior, dan dewan pengawas?

- Tentukan apa tanggung jawab pengguna, termasuk manajemen senior, mengoperasikan sistem secara aman?
- Beberapa sering anda memeriksa virus pada sistem deskop dan laptop anda?
- Apa yang anda lakukan jika menemukan virus?
- Bagaimana anda memulihkan file yang terkompromi?
- Bagaimana anda melokalisir kerusakan yang disebabkan oleh virus?
- Bagaimana mencegah penyebaran virus ke komputer/sistem lain?
- Bagaimana meverifikasi bahwa file yang baru dibuat tidak terkontaminasi?
- Apa administrator secara regular memeriksa keberadaan virus, worm, Trojan horse, dan denial-of-service agents?

PEDOMAN NO. 6.3

Manajemen sistem &jaringan : konfigurasi aset aman

Siapkan prosedur dan akan mekanisme untuk memastikan konfigurasi aman dari semua asset terpasang sepanjang siklus kehidupan dari instalasi, operasi, pemeliharaan, dan penonaktifkannya (detil selanjutnya, lihat [1].)

Lakukan patches untuk memperbaiki masalah keamanan dan fungsionalitas.

Buat dan jaga satu standar, konfigurasi esensiel minimum untuk setiap tipe computer dan setiap jenis layanan.

Buat diagram topologi jaringan dan pastikan selalu up-to-date.

Aktifkan level logging yang memadai.

Perhatikan implikasi keamanan untuk semua perubahan terhadap sistem dan jaringan.

Lakukan asesmen kerawanan secara periodic dan tangani kerawanan yang diketemukan.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Bagaimana anda tahu bahwa konfigurasi desktop dan laptop anda dan server yang anda akses aman sebagaimana mestinya? Kepada siapa anda bertanya?
- Bagaimana anda ketahui tentang update yang diperlukan dan software kritis? Bagaimana anda tahu tentang kemajuan instalasi perubahan pada infrastuktur perusahaan anda?
- Bolekah pengguna download software mereka sendiri dari rumah?

PEDOMAN NO. 6.4

Manajemen sistem &jaringan : backups

Lakukan skedul backup regular untuk software dan data.

Vaslidasi software dan data sebelum backup

Vaslidasi software dan data sesudah backup

Vertifikasi kapasitas pemulihan dari backups

Hal-hal yang harus diperhatikan pimpinan, manajer senior, dan dewan pengawas?

- Apa yang anda lakukan ketika akan meretrieve file backup yang secara tidak sadar telah anda hapus? Beberapa lama ini makan waktu?
- Apa peran anda dalam mem-backup data pengguna dalam desktop dan laptop anda?

PEDOMAN NO. 7: otentikasi & otorisasi

PEDOMAN NO. 7.1

Otentikasi & otorisasi: pengguna

Terapkan dan pelihara mekanisme yang memadai untuk otentikasi dan otorisasi pengguna ketika menggunakan akses jaringan dari dalam dan luar organisasi.

Pastikan ini konsisten dengan kebijakan, prosedur, peran, dan level pembatasan akses yang diperlukan untuk asset spesifik (juga lihat pedoman no. 6.1)

Hal-hal yang harus diperhatikan pimpinan, manajer senior, dan dewan pengawas?

- Sarana identifikasi dan otentikasi apa yang diperlukan untuk mengakses sistem yang anda gunakan setiap hari? Juga untuk mengakses sistem yang

lebih kritis dan terproteksi yang mungkin perlu digunakan sewaktu-waktu?

- Jika tidak tahu, kepada siapa anda bertanya?

PEDOMAN NO. 7.2

Otentikasi &otorisasi : rimut dan pihak ketiga

Lindungi aset kritis ketika memberikan akses jaringan kepada pengguna yang bekerja secara rimut dan kepada pihak ketiga seperti kontraktor dan penyedia layanan.

> *Gunakan jaringan, sistem-, file-, dan level aplikasi control akses dan batasi akses pada waktu dan tugas yang diotorisasi, dimana diperlukan. (juga lihat pedoman no. 6.1)*
>
> *Gunakan enkripsi data dan teknologi VPN, di mana diperlukan.*

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Bagaimana mengakses jaringan dan sistem organisasi ketika anda bekerja dari rumah atau dalam perjalanan? Apakah anda boleh dial-up langsung ke modem yang tersambung ke desktop atau server?
- Apakah akses anda dibatasi dibanding ketika anda bekerja dikantor?
- Apakah anda memiliki proses untuk memutuskan dan prosedur pendukung yang memberi akses pihak ketiga, mengelola setiap jenis hubungan dengan level keamanan tertentu, dan menutup atau meng-update account ketika kerjasama dihentikan?
- Jika tidak, kepada siapa bertanya?

PEDOMAN NO. 8

Pengawasan & audit

Gunakan pengawasan yang memadai, pemeriksaan, dan fasilitas inspeksi dan tanggung jawab penugasan untuk melapor, mengevaluasi, dan merespons terhadap kejadian dan kondisi sistem dan jaringan.

Gunakan perangkat pengawasan sistem dan jaringan secara regular dan periksa hasil kerjanya.

Gunakan filter dan perangkat analisis dan periksa hasil kerjanya.

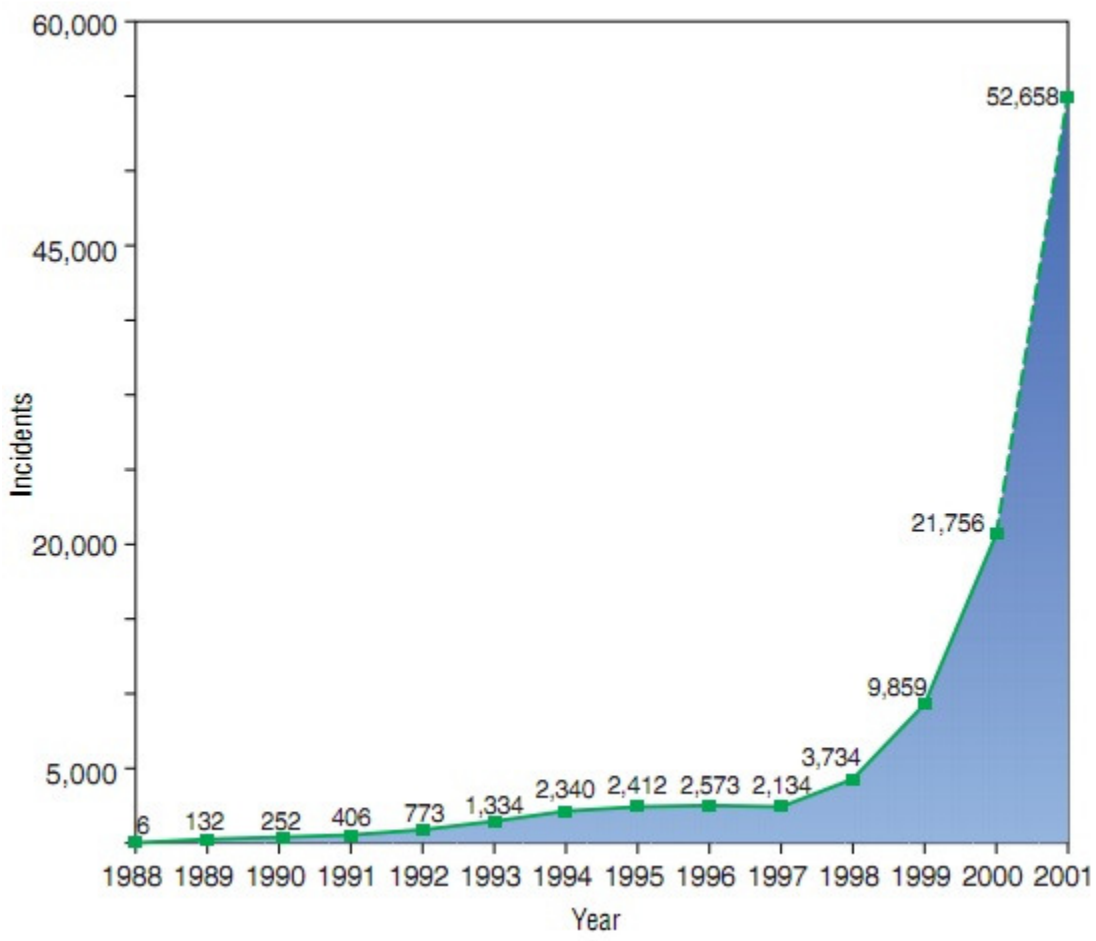
Tanggap atas kejadian yang membutuhakan langkah responsive.

Pastikan semua karyawan tahu siapa yang harus dihubungi ketika mereka menemukan hal-hal yang mencurigakan.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Ketika sesuatu nampak mencurigakan dalam sistem anda, siapa yang anda hubungi dan informasi apa yang anda perlukan untuk mendeskripsikan permasalahannya?
- Apakah sistem anda pernah kebobolan? Bagaimana anda tahu?
- Siapa yang anda hubungi untuk mengetahui bagaimana email dan akses web anda diawasi?
- Adakah sistem dan admin jaringan anda memiliki daftar kontak aktif untuk jaringan primer dengan mana anda berinterface?
- Apakah admin anda up-to-date atas ancaman, serangan, dan solusi terakhir? Sumber daya apa yang mereka gunakan?

Insiden keamanan telah meningkat lebih dari dua kali lipat setiap tahun sejak 1988. Ekonomis computer dari Carlsbad, California memperkirakan bahwa virus red code – satu insiden tunggal – telah menyebabkan kerugian $ 1,1 milyar dalam hilangnya produktivitas.



PEDOMAN NO. 9

Keamanan fisik

Control akses fisik pada asset informasi dan layanan serta sumber daya TI.

Gunakan control akses fisik (yaitu badges, biometrics, kunci), dimana perlu.
Gunakan kunci elektronik dengan password untuk terminal kerja, server, dan laptop yang aktif saat login dan sesudah non aktif beberapa saat.
Control akses ke semua aset perangkat keras kritis (yaitu routers, firewalls, server, hub mail).

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Sarana identifikasi dan otentikasi apa yang anda perlukan untuk mengakses fasilitas primer dikantor anda? Fasilitas kritis yang anda perlu kunjungi setiap saat?
- Jaminan apa yang anda dapat bahwa pembatasan akses fisik diikuti? Bagaimana pelanggaran dilaporkan kepada anda?
- Tahukah anda siapa yang harus dihubungi jika anda menemukan surat, paket, atau barang lain yang mencurigakan dikirim dengan pos atau layanan kiriman? Apa yang anda anggap sebagai mencurigakan?

PEDOMAN NO. 10

Rencana kontinyuitas & pemulihan bencana

Buat rencana kontinyuitas bisnis dan pemulihan bencana untuk aset kritis dan lakukan tes secara periodik dan pastikan berfungsi efektif.

Hal-hal yang harus diperhatikan pimpinan, manajer senior dan dewan pengawas?

- Apakah anda memiliki rencana kepastian misi yang menjamin kontinyuitas bisnis dan operasi dan pemulihan bencana? Apakah rencana ini dites secara

regular dan dijamin efektif?

- Jika akses ke fasilitas ke fasilitas e-commerce internet di perusahaan anda hilang 4-5 hari, akankah dampaknya menyebabkan ketidak-stabilan finansial?
- Apa yang anda lakukan dan siapa yang anda hubungi ketika terjadi kebakaran pada fasilitas anda?
- Siapa yang anda hubungi jika terjadi bencana alam untuk menentukan bagaimana memenuhi tanggung jawab pekerjaan anda?
- Bagaimana anda berfungsi efektif jika jaringan anda biasanya bekerja, tidak tersedia?

Catatan akhir

Rekomendasi ini mencoba menanggapi pedoman keamanan untuk sistem dan jaringan oprasional yang tergelar saat ini dan memberikan satu perspektif manajeman top-down yang dapat digunakan untuk mengakses postur keamanan informasi suatu organisasi.

Kami sarankan pembaca untuk menyebarkan buku ini seluas-luasnya guna membantu organisasi mengelola risiko keamanan dan mengadopsi praktek manajemen keamanan yang efektif.Keamanan terus berkembang sebagai masalah yang kritis yang perlu mendapat perhatian di lingkungan komuntas internet. Departemen kominfo akan terus memperbaiki dan mengembangkan pedoman praktis manajemen keamanan informasi untuk pimpinan orgaisasi ini guna memenuhi meningkatnya kebutuhan dan tantangan ancaman kami harapkan partisipasi anda sebagai bagian dari upaya penting ini.

Kami akan sangat menghargai komentar dan tanggapan anda, silahkan kirim e-mail :ksi_ditsiplk@depkominfo.go.id.