BAB 11
TANTANGAN KEAMANAN DAN ETIKA

2 masalah utama tentang keamanan sistem yaitu :

1. Threats (Ancaman) atas sistem dan
2. Vulnerability (Kelemahan) atas sistem

Masalah tersebut pada gilirannya berdampak kepada 6 hal yang utama dalam sistem informasi yaitu :

- Efektifitas
- Efisiensi
- Kerahaasiaan
- Integritas
- Keberadaan (availability)
- Kepatuhan (compliance)
- Keandalan (reliability)

Untuk menjamin hal tersebut maka keamanan sistem informasi baru dapat terkriteriakan dengan baik. Adapun kriteria yag perlu di perhatikan dalam masalah keamanan sistem informasi membutuhkan 10 domain keamanan yang perlu di perhatikan yaitu :

1. Akses kontrol sistem yang digunakan
2. Telekomunikasi dan jaringan yang dipakai
3. Manajemen praktis yang di pakai
4. Pengembangan sistem aplikasi yang digunakan
5. Cryptographs yang diterapkan
6. Arsitektur dari sistem informasi yang diterapkan
7. Pengoperasian yang ada
8. Busineess Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
9. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan
10. Tata letak fisik dari sistem yang ada

Dari domain tersebutlah isu keamanan sistem informasi dapat kita klasifikasikan berdasarkan ancaman dan kelemahan sistem yang dimiliki.

ANCAMAN (Threats)

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu :

1. Ancaman Alam
2. Ancaman Manusia
3. Ancaman Lingkungan

Ancaman Alam

Yang termasuk dalam kategori ancaman alam terdiri atas :

- Ancaman air, seperti : Banjir, Stunami, Intrusi air laut, kelembaban tinggi, badai, pencairan salju
- Ancaman Tanah, seperti : Longsor, Gempa bumi, gunung meletus
- Ancaman Alam lain, seperti : Kebakaran hutan, Petir, tornado, angin ribut

Ancaman Manusia

Yang dapat dikategorikan sebagai ancaman manusia, diantaranya adalah :

- Malicious code
- Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasures
- Social engineering
- Hacking, cracking, akses ke sistem oleh orang yang tidak berhak, DDOS, backdoor
- Kriminal
- Pencurian, penipuan, penyuapan, pengkopian tanpa ijin, perusakan
- Teroris
- Peledakan, Surat kaleng, perang informasi, perusakan

Ancaman Lingkungan

Yang dapat dikategorikan sebagai ancaman lingkungan seperti :

- Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama
- Polusi
- Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll
- Kebocoran seperti A/C, atap bocor saat hujan

Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu di klasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat di minimalisir dengan pasti. Setiap ancaman tersebut memiliki probabilitas serangan yang beragam baik dapat terprediksi maupun tidak dapat terprediksikan seperti terjadinya gempa bumi yang mengakibatkan sistem informasi mengalami mall function.

KELEMAHAN (Vurnerability)

Adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut. Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti : Seting firewall yang membuka telnet sehingga dapat diakses dari luar, atau Seting VPN yang tidak di ikuti oleh penerapan kerberos atau NAT.

Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu :

1. Pendekatan *preventif* yang bersifat mencegah dari kemungkinan terjadikan ancaman dan kelemahan

2. Pendekatan *detective* yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal
3. Pendekatan *Corrective* yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

Tindakan tersebutlah menjadikan bahwa keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, mallware, spy ware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

TANTANGAN KEAMANAN DAN ETIKA TI

Penggunaan TI dalam bisnis memiliki dampak besar pada masyarakat danakhirnya akan menimbulkan berbagai isu etika dalam hal kejahatan, privasi, individualitas dan lainnya. TI dapat memiliki hasil yang bermanfaat dan juga merusak pada masyarakat serta pihak-pihak disetiap area ini.

TANGGUNG JAWAB ETIKA DARI PROFESSIONAL BISNIS

praktisi bisnis memiliki tanggung jawab untuk menyebarluaskan penggunaan TI yang beretika di tempat kerja. Seorang manajer ataupun praktisi bisnis bertanggung jawab membuat keputusan mengenai berbagai aktivitas bisnis dan penggunaan TI, yang mungkin memiliki dimensi etika yang harus dipertimbangkan.

Contohnya :

- ❖ Haruskah praktisi bisnis secara elektronik memonitor aktivitas kerja para karyawan dan email mereka.
- ❖ Haruskah membiarkan karyawan menggunakan komputer di tempat kerja mereka untuk kepentingan pribadi atau membawa pulang berbagai copy software untuk digunakan sendiri.

- ❖ Haruskah secara elektronik mengakses catatan pribadi karyawan atau berbagai file ditempat kerja karyawan
- ❖ Haruskah menjual informasi pelanggan yang di ekstrasi dari sistem pemrosesan transaksi ke perusahaan lain

Etika bisnis (business ethics) berkaitan dengan berbagai pertanyaan etika yang harus dihadapi para manajer dalam pengambilan keputusan mereka sehari-hari. Teori stakeholder (stakeholder theory) dalam etika bisnis menekankan bahwa para manajer memiliki tanggung jawab etika untuk mengelola perusahaan demi kebaikan semua pemilik kepentingan, yang terdiri dari individu atau kelompok dengan kepentingan atau kebutuhan atas perusahaan. Hal ini biasanya meliputi para pemegang saham perusahaan, karyawan, pelanggan, pemasok, dan masyarakat setempat. Kadang kala istilah tersebut diperluas dengan memasukkan semua kelompok yang dapat mempengaruhi atau dipengaruhi oleh perusahaan, seperti pesaing, lembaga pemerintahan dan kelompok kepentingan khusus. Selain etika bisnis ada juga yang disebut sebagai etika teknologi (technology ethics). Prinsip-prinsip etika teknologi, yaitu:

- ❖ Proporsional. Hal baik yang dicapai melalui teknologi harus melebihi bahaya atau risikonya. Bahkan, harus ada alternatif yang dapat mencapai manfaat yang sama atau yang sebanding dengan bahaya atau risiko yang lebih kecil.
- ❖ Persetujuan Berdasarkan informasi. Mereka yang terkena dampak dari teknologi harus memahami dan menerima berbagai risikonya.
- ❖ Keadilan. Manfaat dan beban teknologi harus disebarkan secara adil. Mereka yang mendapat manfaat menanggung bagian yang adil risikonya, dan mereka yang tidak mendapatkan manfaat harus di bebaskan dari penderitaan akibat peningkatan risiko yang signifikan.
- ❖ Minimalisasi Risiko. Bahkan jika dinilai dapat diterima oleh ketiga petunjuk diatas, teknologi harus diimplementasikan dengan sedemikian rupa untuk menghindari semua risiko yang tidak perlu ada.

KEJAHATAN KOMPUTER

Kejahatan dunia maya adalah ancaman yang berkembang bagi mayarakat, yang disebabkan oleh penjahat atau tindakan yang tidak bertanggung jawab dari para individual yang mengambil keuntungan dari penggunaan luas serta kerentanan komputer dan internet, serta jaringan lainnya. Kejahatan komputer (computer crime) didefinisikan oleh Association of Information Technology Professionals (AITP) meliputi :

1. Penggunaan, akses, modifikasi, dan pengaturan hardware, software, data atau sumber daya jaringan secara tidak sah
2. pemberian informasi secara tidak sah
3. pembuatan copy software secara tidak sah
4. mengingkari akses pemakai akhir ke hardware, software, data, atau sumber daya jaringan sendiri
5. Menggunakan atau berkonspirasi untuk menggunakan sumber daya komputer atau jaringan untuk secara illegal mendapatkan informasi atau properti berwujud.

Hacking adalah penggunaan komputer yang obsesif, atau akses dan penggunaan tidak sah dalam sistem jaringan komputer.

Taktik umum hacking yaitu:

- Pengingkaran Layanan (Denial of Service) Praktik ini menjadi hal yang umum dalam permainan jaringan. Dengan menghujani perlengkapan situs web dengan terlalu banyak permintaan, penyerang dapat secara efektif menyumbat sistem, memperlambat kinerja atau bahkan merusak situs tersebut. Metode membebani komputer secara berlebihan ini kadang kala digunakan untuk menutupi serangan.
- Memindai (Scans) Penyebaran pemeriksaan internet untuk menetapkan jenis komputer, layanan, dan koneksinya. Melalui cara itu para penjahat

dapat memanfaatkan kelemahan dalam program komputer atau software tertentu.

- Pengendus (Sniffer) Program yang secara terbalik mencari setiap paket data ketika mereka melalui internet, menangkap password atau keseluruhan isi paketnya.
- Memalsu (Spoofing) Memalsu alamat email atau halaman web untuk menjebak pemakai menyampaikan informasi penting seperti password atau nomor kartu kredit.
- Kuda Troya (Trojan Horse) program yang tanpa diketahui pemakai, berisi perintah untuk memanfaatkan kerentanan yang diketahui dalam beberapa software.
- Pintu Belakang (Back Door) Jika titik masuk asli telah dideteksi, membuat beberapa cara kembali mudah dan sulit untuk dideteksi.
- Applet Jahat (Malicious Applets) Program mini, kadang kala ditulis dalam bahasa komputer yang terkenal, Java, yang menyalahgunakan sumber daya komputer anda, mengubah file di hard disk, mengirim email palsu, atau mencuri password.
- War Dialling Program yang secara otomatis menelepon ribuan nomor telepon melalui koneksi modem
- Bom Logika (Logic Bomb) Perintah dalam program komputer yang memicu tindakan jahat.
- Pembebanan Penyimpanan sementara (buffer Overflow) Tekhnik untuk merusak atau mengambil alih kendali komputer dengan mengirimkan terlalu banyak data ke area penyimpanan sementara komputer di memori komputer.
- Penjebol Password (Password Cracker) Software yang dapat menebak password.
- Rekaya social (Social Engineering) Taktik yang digunakan untuk mendapatkan akses ke sistem komputer melalui perbincangan dengan para

karyawan perusahaan yang tidak menaruh curiga untuk mengorek informasi berharga seperti password.

- Penyelaman Bak Sampah (Dumpster Diving) Berburu melalui sampah perusahaan untuk menemukan informasi yang membantu menerobos masuk ke dalam komputer perusahaan tersebut. Kadang kala informasi tersebut digunakan untuk membuat jebakan dalam rekayasa melalui kehidupan sosial, lebih kredibel.

Beberapa contoh penyalahgunaan internet di tempat kerja:

- Penyalahgunaan umum email
- Penggunaan dan akses tidak sah seperti berbagi password dan akses ke dalam jaringan tanpa ijin
- Pelanggaran / pemalsuan hak cipta
- Memasukkan pesan mengenai berbagai topik yang tidak terkait dengan pekerjaan ke newsgroup
- Transmisi data rahasia seperti penggunaan internet untuk menampilkan atau mentransmisikan rahasia dagang
- Pornografi
- Hacking
- Download / upload hal-hal yang tidak berkaitan dengan pekerjaan
- Penggunaan internet untuk hiburan
- Penggunaan ISP eksternal untuk terhubung dengan internet agar dapat menghindari deteksi
- Menggunakan sumber daya kantor untuk kerja sampingan

TANTANGAN KEAMANAN OPERASI E-BUSINESS

Tantangan keamanan teknologi informasi dalam operasi e-business mencangkup masalah keleluasaan pribadi. Masalah keleluasan pribadi yang diperdebatkan dalam dunia bisnis dan pemerintah meliputi :

1. Pelanggaran keleluasaan pribadi

Mengakses percakapan e-mail pribadi dan atau mengumpulkan dan menyebarkan informasi tentang individu tanpa pengetahuan atau persetujuan mereka

2. File pribadi yang tidak sah

   Mengumpulkan nomor telepon, nomor kartu kredit, alamat e-mail, dan informasi lain yang bersifat pribadi untuk membangun suatu profil pelanggan individu

3. Memantau komputer

   Menggunakan teknologi untuk memonitor percakapan, produktivitas karyawan atau suatu kegiatan individual

4. Mempertemukan komputer

   Menggunakan informasi pelanggan yang diperoleh dari berbagai sumber untuk menciptakan suatu profil pelanggan yang dapat dijual kepada perantara informasi atau perusahaan lain dan sebagai jasa bisnis lain.

5. Perlindungan keleluasaan pribadi pemakai

   Hukum mengenai keleluasaan pribadi mencoba untuk menanggulangi sebagian dari masalah ini. Ketentuan mengenai komunikasi pribadi secara elektronik dan ketentuan tentang penipuan dan tindakan penyalahgunaan melalui komputer, melarang seseorang untuk menginterupsi pesan komunikasi data, mencuri atau membinasakan data. Ketentuan tentang mempertemukan komputer dan tindakan keleluasaan pribadi mengatur tentang mempertemukan data disimpan dalam file agen pemerintah pusat. Individu dapat juga melindungi keleluasaan pribadi mereka dengan penggunaan perangkat lunak dan jasa seperti encryption dan email tanpa nama.

Berbagai isu privasi

Isu mengenai privasi yang penting sedang di perdebatkan dalam dunia bisnis dan pemerintah. Karena teknologi internet mempercepat semua keberadaan koneksi telekomunikasi global dalam bisnis dan masyarakat. Contohnya :

- ❖ Mengakses percakapan pribadi email seseorang dan catatan komputernya, serta mengumpulkan dan berbagi informasi mengenai keuntungan individual yang didapat dari kunjungan mereka pada berbagai situs web internet serta newsgroup.
- ❖ Selalu mengetahui lokasi seseorang terutama ketika telepon genggam menjadi makin erat dihubungkan dengan orang dari pada tempat.
- ❖ Menggunakan informasi pelanggan yang didapatkan dari banyak sumber untuk memasarkan layanan bisnis tambahan.
- ❖ Mengumpulkan nomor telepon, alamat email, nomor kartu kredit, dan informasi personal lainnya untuk membangun profil setiap pelanggan.

Berbagai isu kesehatan

Penggunaan TI di tempat kerja meningkatkan berbagai isu kesehatan (health issue). Penggunaan yang intensif atas komputer dilaporkan menyebabkan masalah kesehatan seperti stress di tempat kerja, kerusakan otot tangan dan leher, kelelahan mata, ekspos terhadap radiasi dan bahkan kematian oleh kecelakaan yang disebabkan oleh komputer.

Solusi untuk beberapa masalah kesehatan ini didasarkan pada ilmu ergonomic (ergonomics), yang kadang disebutkan sebagai rekayasa faktor manusia (human factors engineering). Tujuan dari ergonomik adalah untuk mendesain lingkungan kerja sehat yang aman, nyaman dan menyenangkan bagi orang-orang untuk bekerja didalamnya, hingga meningkatkan moral serta produktivitas karyawan. Ergonomik menekankan pada kesehatan desain tempat kerja, terminal kerja, komputer dan mesin lainnya, bahkan paket software. Masalah kesehatan lainnya mungkin membutuhkan solusi ergonomic yang menekankan pada desain pekerjaan, daripada desain tempat kerja.

MANAJEMEN KEAMANAN TI

Tujuan dari manajemen keamanan (security management) adalah untuk akurasi, integritas dan keamanan proses serta sumber daya semua sistem informasi.

Manajemen keamanan yang efektif dapat meminimalkan kesalahan, penipuan dan kerugian dalam SI yang saling menghubungkan perusahaan saat ini dengan para pelanggan, pemasok dan stakeholder lainnya.

Beberapa pertahanan yang penting saat ini :

- Enkripsi data
- Firewall
- Pertahanan dari serangan pengingkaran layanan (distributed denial of service)

  Serbuan pengingkaran layanan melalui internet tergantung pada 3 lapis sistem komputer jaringan, yaitu:

  a. Situs web korban
  b. Penyedia layanan internet korban
  c. Situs "zombie" atau komputer bantuan yang diaktifkan oleh para penjahat dunia maya.
- Pemonitoran email
- Pertahanan dari virus

Beberapa alat keamanan lainnya, yaitu:

- Kode keamanan

  Biasanya sistem password bertingkat digunakan untuk manajemen keamanan
- Pembuatan cadangan file (backup file)
- Pemonitor keamanan

  Keamanan suatu jaringan dapat disediakan oleh paket software sistem khusus yang disebut sebagai pemonitor keamanan sistem (system security monitor)
- Keamanan biometris (biometric security)

  Merupakan alat keamanan yang disediakan oleh peralatan komputer, yang mengukur ciri khas fisik yang membedakan setiap individu. Hal ini meliputi verifikasi suara, sidik jari, geometri tangan, dinamika tanda

tangan, analisis penekanan tombol, pemindai retina mata, pengenalan wajah, serta analisis pola genetik.

- ❖ Pengendali kegagalan komputer
- ❖ Sistem toleransi kegagalan (fault tolerant)
- ❖ Pemulihan dari bencana (disaster recovery)

PENGENDALIAN DAN AUDIT SISTEM

Dua persyaratan akhir manajemen keamanan adalah pengembangan pengendalian SI dan penyelesaian audit sistem bisnis.

Pengembangan pengendalian SI (information system controls) Adalah metode dan alat yang berusaha untuk memastikan akurasi, validitas, dan kebenaran aktivitas SI. Pengendalian SI harus dikembangkan untuk memastikan entri data, teknik pemrosesan, metode penyimpanan, serta output informasi yang tepat. Jadi, pengendalian SI didesain untuk memonitor dan memelihara kualitas serta keamanan input, pemrosesan, output, dan aktivitas penyimpanan di sistem informasi mana pun.

Penyelesaian audit sistem bisnis

Manajemen keamanan TI harus secara periodik diperiksa, atau diaudit, oleh karyawan bagian internal audit di perusahaan atau auditor eksternal dari kantor akuntan public professional. Audit semacam ini mengkaji dan mengevaluasi apakah alat keamanan dan kebijakan manajemen yang memadai telah dikembangkan serta diimplementasikan. Hal ini biasanya meliputi verifikasi akurasi dan integritas software yang di gunakan, serta input data dan output yang dihasilkan oleh berbagai aplikasi bisnis. Tujuan penting lainnya dari audit sistem bisnis adalah menguji integritas dari jejak audit aplikasi. Jejak audit (audit trail) dapat didefinisikan sebagai keberadaan dokumentasi yang memungkinkan sebuah transaksi ditelusuri melalui berbagai tahapan pemrosesan informasinya.