PERTEMUAN 11

KEAMANAN SISTEM INFORMASI DAN ETIKA

A. TUJUAN PEMBELAJARAN

Melalui risetasi, mahasiswa diharapkan mampu:

1.1 Memahami konsep teknologi informasi, input/output, dan prosesnya.

1.2 Mampu melakukan teknik penyimpanan data dan bisa mengenal serta mengendalikan berbagai virus-virus komputer.

1.3 Mengetahui batas-batas *cyberlaw* dan penerapannya.

B. URAIAN MATERI

1.1 Kontrol Sistem Informasi

1.2 Pengendalian Input, Proses, Dan Output

1.3 Pengendalian Penyimpanan

1.4 Pengenalan Virus Komputer

Karena berbicara tentang keamanan Sistem Informasi maka yang satu ini tidak boleh dilupakan yaitu virus. Virus Komputer adalah program yang mengganggu sistem kerja komputer, sehingga dapat menyebabkan komputer sering *hang*, lelet, *bluescreen*, bahkan sampai-sampai untuk mengatasinya kita harus melakukan instal ulang komputer kita. Berikut macam-macam virus:

1. Virus Compiler

Virus yang sudah di compile sehingga dapat dieksekusi langsung. Ini adalah virus yang pertama kali muncul di dunia komputer, dan mengalami perkembangan pesat sekarang. Virs pertama ini sangatlah sulit dibasmi karena dibuat dengan bahasa rendah, assembler. Memang bahasa ini cocok untuk membuat virus namun sangatlah susah menggunakannya. Keunggulan dari virus ini adalah mampu melakukan hampir seluruh manipulasi yang mana hal ini tidak selalu dapat dilakukan oleh virus jenis lain karena lebih terbatas.

2. Virus Bagle BC

Virus ini ini termasuk salah satu jenis virus yang berbahaya dan telah masuk peringkat atas jenis virus yang paling cepat mempengaruhi komputer kita. Beberapa jam sejak keluarnya virus ini, sudah terdapat 2 buah varian Bagle (Bagle BD dan BE) yang menyebar melalui e-mail, jaringan komputer dan aplikasi P2P. Virus ini menyebar melalui e-mail dengan berbagai subyek berbeda. Menurut suatu penelitian dari Panda Software virus Bagle BC ini menyusup ke dalam e-mail dengan subyek antara lain : Re:, Re:Hello, Re:Hi, Re:Thank you, Re:Thanks. Attachment-nya juga bermacam-macam, antara lain : .com, .cpl, .exe, .scr. Virus Bagle BC juga mampu untuk menghentikan kerja program-program antivirus.

3. Virus File

Adalah virus yang memanfaatkan file yang dapat diijalankan/dieksekusi secara langsung. Biasanya file *.EXE atau *.COM. Tapi bisa juga menginfeksi file *.SYS, *.DRV, *.BIN, *.OVL dan *.OVY. Jenis Virus ini dapat berpindah dari satu media ke semua jenis media penyimpanan dan menyebar dalam sebuah jaringan.

4. Virus Sistem

Atau lebih dikenal sebagai virus Boot. Kenapa begitu karena virus ini memanfaatkan file-file yang dipakai untuk membuat suatu sistem komputer. Sering terdapat di disket/tempat penyimpanan tanpa sepengetahuan kita. Saat akan menggunakan komputer (restart), maka virus ini akan menginfeksi Master Boot Sector dan System Boot Sector jika disket yang terinfeksi ada di drive disket/tempat penyimpanan.

5. Virus Boot Sector

Virus yang memanfaatkan hubungan antar komputer dan tempat penyimpanan untuk penyebaran virus. Apabila pada boot sector terdapat suatu program yang mampu menyebarkan diri dan mampu tinggal di memory selama komputer bekerja, maka program tersebut dapat disebut virus. Virus boot sector

terbagi dua yaitu virus yang menyerang disket dan virus yang menyerang disket dan tabel partisi.

6. Virus Dropper

Suatu program yang dimodifikasi untuk menginstal sebuah virus komputer yang menjadi target serangan. setelah terinstal, maka virus akan menyebar tetapi Dropper tidak ikut menyebar. Dropper bisa berupa nama file seperti Readme.exe atau melalui Command.com yang menjadi aktif ketika program berjalan. Satu program Dropper bisa terdapat beberapa jenis Virus.

7. Virus Script/Batch

Awalnya virus ini terkenal dengan nama virus batch seperti yang dulu terdapat di file batch yang ada di DOS.Virus script biasanya sering didapat dari Internet karena kelebihannya yang fleksibel dan bisa berjalan pada saat kita bermain internet, virus jenis ini biasanya menumpang pada file HTML (Hype Text Markup Language) dibuat dengan menggunakan fasilitas script seperti Javascript, VBscript,4 maupun gabungan antara script yang mengaktifkan program Active-X dari Microsoft Internet Explorer.

8. Virus Macro

Virus yang dibuat dengan memanfaatkan fasilitas pemrograman modular pada suatu program aplikasi seperti Ms Word, Ms Excel, Corel WordPerfect dan sebagainya. Walaupun virus ini terdapat didalam aplikasi tertentu tetapi bahaya yang ditimbulkan tidak kalah berbahanya dari virus-virus yang lain.

9. Virus Polymorphic

Dapat dikatakan virus cerdas karena virus dapat mengubah strukturnya setelah melaksanakan tugas sehingga sulit dideteksi oleh Antivirus.

10. Virus Stealth

Virus ini menggunakan cara cerdik, yakni dengan memodifikasi struktur file untuk meyembunyikan kode program tambahan di dalamnya. Kode ini memungkinkan virus ini dapat menyembunyika diri. Semua jenis virus lain juga memanfaatkan kode ini. Ukuran-ukuran file tidak berubah setelah virus menginfeksi file.

11. Virus Companion

Virus jenis ini mencari file *.EXE untuk membuat sebuah file *.COM dan menyalin untuk meletakkan virus. Alasannya, file *.COM berjalan sebelum file *.EXE.

12. Worm

Adalah sebuah program yang bersifat parasit karena dapat menduplikasi diri. Akan tetapi, worm tidak menyerupai virus karena tidak menginfeksi program komputer lainnya. Oleh karena itu, Worm tidak digolongkan ke dalam virus. Mainframe adalah jenis komputer yang sering diserang Worm. Penyebarannya pada komputer lainnya melalui jaringan. Dalam perkembangannya Worm mengalami “mutasi genetik” sehingga selain membuat suatu file baru, ia pun akan berusaha menempelkan dirinya sendiri ke suatu file, ini biasa disebut virus Hybrid.

13. Virus Hybrid

Virus ini merupakan virus yang mempunyai dua kemampuan biasanya dapat masuk ke boot sector dan juga dapat masuk ke file. Salah satu contoh virus ini adalah virus Mystic yang dibuat di Indonesia.

14. Trojan horse

Disebut juga kuda troya. Trojan menginfeksi komputer melalui file yang kelihatannya tidak berbahaya dan biasanya justru tampaknya melakukan sesuatu yang berguna. Namun akhirnya virus menjadi berbahaya, misalnya melakukan format hardisk.

15. Backdoor Alnica

Virus yang juga berbahaya ini merupakan salah satu tipe virus Trojan Horse. Merupakan salah satu virus backdoor yang jika berhasil menginfeksi komputer akan mampu melakukan akses dari jarak jauh dan mengambil segala informasi yang diinginkan oleh si penyerang. Sistem operasi yang diserang oleh virus tersebut antara lain : Windows 200, Windows 95, Windows 98, Windows Me, Windows NT dan Windows XP. Virus ini berukuran sebesar 57.856 byte

16. Trojan di Linux

Para pengguna linux Red Hat diharapkan untuk berhati-hati terhadap PATCH yang dikirm melalui e-mail dengan alamat "security@redhat.com" karena itu sebenarnya bukannya patch security tetapi virus Trojan yang bisa mengacaukan sistem keamanan. E-mail peringatan dari Red Hat biasanya selalu dikirim dari alamat "secalert@redhat.com" dan ditandatangani secara digital. Virus ini juga pernah menyerang sistem keamanan Windows tahun 2003 dengan subyek menawarkan solusi keamanan.

Nah, rupanya di Linux juga bisa kena virus. Inilah salah satu akibat perkembangan teknologi. Mulai sekarang, semakin berhati-hatilah dan jangan sembarangan mengcopy sebuah file dari source lain lalu di-paste ke komputer anda. Jangan lupa rajin mengupdate antivirus untuk meningkatkan security komputer.

1.5 Etika dan Hukum IT

Etika dalam sistem informasi

Masalah etika juga mendapat perhatian dalam pengembangan dan pemakaian system informasi. Masalah ini diidentifikasi oleh Richard Mason pada tahun 1986 yang mencakup privasi, akurasi, properti, dan akses, yang dikenal dengan akronim PAPA.

1. Privasi

Privasi menyangkut hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang tidak diberi izin unruk melakukannya.

Contoh isu mengenai privasi sehubungan diterapkannya system informasi adalah pada kasus seorang manajer pemasaran yang ingin mengamati *e-mail* yang dimiliki para bawahannya karena diperkirakan mereka lebih banyak berhubungan dengan *e-mail* pribadi daripada *e-mail* para pelanggan. Sekalipun sang manajer dengan kekuasaannya dapat melakukan hal seperti itu, tetapi ia telah melanggarprivasi bawahannya.

Privasi dibedakan menjadi privasi fisik dan privasi informasi (Alter, 2002). Privasi fisik adalah hak seseorang untk mencegah ssesеorang yang tidak dikehendaki terhadap waktu, ruang, dan properti (hak milik), sedangkan privasi informasi adalah hak individu untuk menentukan kapan, bagaimana, dan apa saja informasi yang ingin dikomunikasikan dengan pihak lain.

Penggunaan teknologi informasi berkecenderungan membuat pelanggaran terhadap privasi jauh lebih mudah terjadi. Sebagai contoh, para pemakai *e-mail*sering kali jengkel dengan kiriman-kiriman *e-mail* yang tak dikehendaki dan berisi informasi yang tidak berguna (*junk e-mail*).

Di America Serikat, masalah privasi diatur oleh undang-undang privasi. Berkaitan dengan hal ini, maka:

- Rekaman-rekaman data tdak boleh digunakan untuk keperluan lain yang bukan merupakan tujuan aslinya tanpa sepengetahuan individu bersangkutan.
- Setiap individu memiliki hak untuk melihat datanya sendiri dan membetulkan rekaman-rekaman yang menyangkut dirinya.

2. Akurasi

Akurasi terhadap informasi merupakan factor yang harus dpenuhi oleh sebuah sistem informasi. Ketidak akurasian informasi dapat menimbulkan hal yang mengganggu, merugikan, dan bahkan membahayakan.

Sebuah kasusakibat kesalahan penghapusan nomor keamanan social dialami oleh Edna Rismeller (Alter, 2002, hal.292). Akibatnya, kartu asuransinya tidak bias digunakan bahkan pemerintah menarik kembali cek pension sebesar $672 dari rekening banknya. Kisah lain dialami oleh para penyewa apartemen di Amerika yang karena sesuatu hal pernah bertengkar dengan pemiliki apartemen. Dampaknya, terdapat tanda tidak baik dalam basis data dan halini membuat mereka sulit untuk mendapatkan apartemen lain. Mengingat data dalam sistem informasi menjadi bahan dalam pengambilan keputusan, keakurasiannya benar-benar harus diperhatikan.

3. Properti

Ada banyak bentuk sistem hukum yang berlaku di dunia dan memiliki bentuk yang berbeda dalam menghadirkan fakta, aturan dan hak tertuduh. Undang-undang yang berhubungan dengan penggunaan komputer secara etis adalah hak milik intelektual serta perilaku kriminal.

Konsep hukum properti intelektual telah didasarkan pada pengenalan hak-hak dasar properti intelektual dan kebijakan yang mendorong penciptaan karya dengan mengakui hak tertentu pembuatnya. Dalam wilayah teknologi informasi, konsep ini penting sekali terutama bagi perlindungan program komputer dan topografi semi konduktor.

Intelektual properti meliputi:

a. Hak Paten

Memberikan pemilik paten hak hukum yang dilaksanakan untuk mengeluarkan orang lain dari praktek penemuan yang memiliki paten untuk periode waktu tertentu. Hukum paten melindungi penemuan dan proses (kegunaan paten). Hak paten diberikan untuk melindungi hak penemu suatu alat fisik.

Paten merupakan bentuk perlindungan terhadap kekayaan intelektual yang paling sulit didapatkan karena hanya akan diberikan pada penemuan-penemuan inovatif dan sangat berguna. Hukum paten memberikan perlindungan selama 20 tahun.

b. Copyright

Melindungi “pekerjaan orisinil kepengarangan”, melindungi hak penulis untuk mengontrol reproduksi, adaptasi, distribusi publik, kinerja karya orisinil ini dapat diaplikasikan ke software dan database. Hal yang harus dipertimbangkan dari sudut hukum ketika menentukan apakah perkecualian pada perlindungan hak cipta diizinkan :

- Tujuan dan sifat penggunaan, mencakup apakah penggunaan itu untuk komersial atau untuk tujuan pendidikan nonprofit
- Sifat karya berhak-cipta
- Jumlah dan substansi bagian yang digunakan dalam hubungannya dengan karya berhak-cipta sebagai suatu keseluruhan
- Efek penggunaan terhadap pasar potensial atau nilai dari karya berhak-cipta.

Jika pengarang karya cetak ingin membuat penjelasan bahwa mereka mempunyai hak cipta, maka mereka harus mencantumkan peringatan. Peringatan hak cipta memasukkan lambing © atau kata Hak Cipta, tahun, dan nama pemilik hak cipta. Hak cipta dimaksudkan untuk melindungi karya cipta selama umur hidup seniman atau pengarang.

Karya cipta yang berada dalam *domain publik* tidak berhak-cipta dan dapat disalin dan disebarkan dengan bebas. Semua karya cipta yang dibuat oleh pemerintah pusat berada dalam domain publik. Karya cipta dapat berada dalam domain publik jika hak ciptanya telah berakhir/kadaluarsa. Hak cipta berakhir setelah 95 tahun.

Sedangkan freeware adalah jenis perangkat lunak yang dimiliki oleh seorang pemilik perangkat lunak berhak-cipta tidak menarik biaya penggunaan. Maksudnya freeware dapat dicopy dan dibagi-bagikan, tetapi tidak boleh direvisi atau dijual ke pihak ketiga.

c. Trade Secret (Rahasia Perdagangan)

Mengamankan dan memelihara kerahasiaan teknis pemilik atau informasi yang berkaitan dengan bisnis yang cukup terlindungi dari penyingkapan oleh pemilik. Akibat wajar terhadap definisi ini adalah bahwa pemiliknya telah

menginvestasikan sumber daya untuk mengembangkan informasi ini, hal ini berharga bagi bisnis pemiliknya, yang berharga bagi pesaing, dan tidak nyata.

d. Trademark

Menyusun kata, nama, simbol, warna, suara, produk, bentuk, device, atau kombinasi ini yang akan digunakan untuk mengidentifikasi produk dan untuk membedakannya dari yang dibuat atau dijual yang lain. Jika seseorang mengklaim bahwa nama atau symbol adalah sebuah merek dagang, mereka mencantumkan singkatan TM. Jika merek dagang secara resmi dikenali dan diregistrasi oleh U.S. Patent and Trademark Office maka nama atau symbol tersebut mempunyai symbol ®. Mencoba menarik keuntungan dari merek dagang orang lain disebut *cybersquatting* praktik ini dinyatakan tidak sah oleh Anticybersquatting Consumer pada tahun 1999.

4. Akses

Fokus dari masalah akses adalah pada penyediaanakses untuk semua kalangan. Teknologi informasi diharapkan tidak menjadi halangan dalam melakukan pengaksesan terhadap informasi bagi kelompok orang tertentu, tetapi justru untuk mendukung pengaksesan untuk semua pihak. Sebagai contoh, untuk mendukung pengaksesan informasi Web bagi orang buta, *TheProducivity Works*(www.prodworks.com) menyediakan Web Broser khusus diberi nama pw WebSpeak. Browser ini memiliki prosesor percakapan dan dapat (Zwass, 1998).

Komputer dapat dilibatkan dalam berbagai jenis perilaku tidak sah, seperti penipuan dan pencurian yang telah ada selama beberapa waktu, tetapi kekuatan komputer, koneksi internetnya, dan anonimitas pengguna telah memberikan piranti baru bagi para penjahat. Kemampuan kompter dan anonimitas pengguna dapat mendorong orang-orang untuk melanggar hukum demi melakukan tindakan illegal. Komunikasi pada internet dapat muncul anonim. Dimana para pengguna dapat memilih untuk menggunakan nama palsu ketika mereka berinteraksi di

internet. Anonimitas seperti ini dapat mendorong kepada perilaku kriminal seperti *cyberstalking* atau *cybersmearing*. *Cyberstalking* meliputi penggunaan internet, e-mail, dan chat rooms untuk menggangu seseorang. *Cybersmearing* adalah penyebaran informasi yang salah yang digunakan untuk merusak reputasi seseorang atau perusahaan.

Komputer juga sangat baik untuk membuat salinan digital berkualitas tinggi dan berbagi salinan tersebut secara elektronis. Praktik seperti ini mempermudah pelanggaran terhadap undang-undang hak cipta dan perjanjian lisensi. Prospek mendapatkan music gratis, video, dan perangkat lunak tanpa membayar loyalty kepada pengarang dan artis merupakan hal menarik bagi banyak orang. Perilaku seperti ini disebut pembajakan perangkat lunak. Perilaku kriminal yang melibatkan penggunaan komputer dapat mudah dilakukan dan sulit untuk penegak hukum untuk mendeteksi hal tersebut. Perilaku tersebut tetap illegal dan tidak etis. Undang-undang pertama mengenai kejahatan komputer yang komprehensif adalah penggelapan komputer dan tindakan penyalahgunaan tahun1986. Undang-undang tersebut merepresentasikan penulisan undang-undang tahun 1984 yang lengkap yang memecahkan permasalahan kejahatan komputer.

Undang-undang kejahatan pidana untuk enam tipe aktivitas komputer :

1. Akses yang tidak terotorisasi terhadap sebuah komputer untuk memperoleh informasi nasional yang rahasia dengan maksud untuk merugikan US atau menguntungkan bangsa asing.
2. Akses yang tidak terotorisasi dari sebuah komputer untuk memperoleh informasi keuangan atau kredit yang dilindungi
3. Akses tidak terotorisasi terhadap komputer yang digunakan pemerintah federal
4. Akses tidak terotorisasi antar negara bagian atau asing dari sebuah sistem komputer dengan maksud menipu
5. Akses sistem komputer yang tidak terotorisasi antara negara bagian atau asing yang menciptakan kerusakan hingga $1000
6. Jual-beli dengan curang menggunakan password komputer yang mempengaruhi perdagangan antara negara bagian.

Sejalan dengan perkembangan teknologi, kejahatan dalam dunia teknologi informasi dan komunikasi (TIK) juga berkembang sangat cepat. Kita tidak akan mungkin dapat menuntaskan semua potensi kejahatan TIK tersebut sekaligus.
Namun ada langkah-langkah reaktif maupun preventif yang dapat dilaksanakan guna mengatasi permasalahan tersebut. Salah satunya melalui penegakan hukum dunia maya *(cyberlaw)*. Oleh karena itu pemerintah memberikan perhatian serius terhadap masalah keamanan informasi. Department Kominfo telah membentuk ID SIRTI (Indonesian Security Incident Response Team on Information Infrastructure), POLRI juga membentuk Cyber Task Force Center.

RUU ITE yang telah lama ditunggu-tunggu kehadirannya, disetujui pemerintah dan DPR dalam rapat paripurna di gedung DPR/MPR, Selasa (25/3). Dari pemerintah, rapat dihadiri Menteri Komunikasi dan Informatika, Moh Nuh, dan Menteri Hukum dan HAM, Andi Matalatta.

Pasal 27

Denda Rp 1 miliar dan enam tahun penjara bagi orang yang membuat, mendistribusikan, mentransmisikan, materi yang melanggar kesusilaan, judi, menghina dan mencemari nama baik, memeras dan mengancam.

Pasal 28

Denda Rp 1 miliar dan enam tahun penjara bagi orang yang menyebarkan berita bohong dan menyesatkan, sehingga merugikan konsumen transaksi elektronik dan menimbulkan kebencian dan permusuhan antarkelompok.

Pasal 30

Denda Rp 800 juta dan penjara 10 tahun bagi orang yang menyadap informasi elektronik atau dokumen elektronik di komputer atau sistem elektronik – mengubah maupun tidak dokumen itu.

Pasal 32

Denda Rp 2-5 miliar dan penjara 8-10 tahun bagi orang yang mengubah, merusak, memindahkan, dan menyembunyikan informasi atau dokumen elektronik.

Pasal 34

Denda Rp 10 miliar dan penjara 10 tahun bagi orang yang memproduksi, menjual, mengimpor, mendistribusikan, atau memiliki perangkat keras dan lunak sebagaimana di Pasal 27-34

Kode Etik

Kode etik merupakan salah satu kontrol bagi penyalahgunaan komputer, tetapi bergantung sepenuhnya hanya dari kode etik bukan merupakan tindakan yang bijaksana, karena kode etik ternyata hanya berpengaruh bagi mereka dengan rasa tanggung-jawab yang tinggi. Agar dapat menerapkan dengan efektif, dukungan dari berbagai pihak sangat diperlukan karena sanksi informal lebih kuat dari sanksi legal.

Secara tidak langsung, kode etik dapat berfungsi sebagaimana layaknya hukum, karena mendefinisikan tindakan-tindakan yang terlarang sehingga membangkitkan kesadaran kepada lingkungannya akan hal tersebut, serta sanksi yang menyertainya.

Keberadaan kode etik khusus IT tidak berpengaruh terhadap penilaian seorang personil IT akan penyalahgunaan komputer. Personil IT dengan '*denial of responsibility*' (RD) rendah cenderung memandang kejahatan komputer sebagai sesuatu yang salah daripada mereka dengan RD tinggi. Personil IT dengan RD tinggi akan cenderung setuju untuk melakukan kejahatan komputer. Kode etik akan meningkatkan ethicality penilaian penyalahgunaan komputer lebih baik pada orang dengan RD tinggi dibandingkan mereka dengan RD rendah. Kode etik akan meningkatkan ethicality niatan penyalahgunaan komputer lebih baik pada orang dengan RD tinggi dibandingkan mereka dengan RD rendah.

Etika Pribadi

Adalah penting untuk mengetahui hukum dan kode etik yang berlaku pada sebuah kelompok khusus, seperti perusahaan, sekolah atau hukum negara. Bagaimanapun, kelompok eksternal tidak selalu menentukan standar perilaku. Saat anda menghadapi berbagai keputusan, anda akan menemukan bahwa beberapa pilihan mudah untuk dibuat, sedangkan yang lain suli, misalnya dilemma moral atas apa yang dilakukan jika anda menemukan seorang teman melakukan sesuatu yang tidak sah. Untuk menghadapi dilema moral. Anda harus mengembangkan etika pribadi. Adalah lebih mudah jika anda memilih *prinsip etika*, yang merupakan ketentuan dasar yang dapat diterapkan untuk situasi-situasi khusus.

Berikut ini prinsip yang membantu anda menentukan apakah suatu tindakan etis atau tidak etis :

- *Jika semua orang bertindak dengan cara yang sama, masyarakat secara keseluruhan akan diuntungkan*. Prinsip ini bermanfaat ketika memutuskan hal-hal yang berhubungkan dengan pembajakan perangkat lunak. Jika semua orang menggunakan musik, video, atau perangkat lunak tanpa membayar royalti, karya kreatif yang baru akan jauh sedikit.
- *Jangan memperlakukan orang sebagai alat untuk mencapai tujuan*. Prinsip ini bermanfaat untuk memilih perilaku anda di ruang chatting atau jenis interaksi lainnya. Tindakan kejam atau menganiaya orang lain untuk membuat diri anda merasa lebih penting merupakan tindakan yang tidak etis menurut prinsip ini.
- *Pengamat yang tidak berat sebelah*. Akan menilai bahwa anda telah bersikap adil kepada semua pihak yang terkait. Penerapan prinsip ini akan membantu anda mempertimbangkan sebuah keputusan dari beberapa sudut pandang dan mempertimbangkan efeknya pada semua pihak.

Jika anda profesional komputer, anda dapat bertanya kepada diri sendiri untuk pertanyaan-pertanyaan ini:

- Apakah anda menyediakan tingkatan keterampilan dan pengetahuan tinggi yang diharapkan dari seseorang di dalam profesi anda?

- Apakah anda menghormati privasi pelanggan? Apakah pelanggan akan marah jika mengetahui anda mengatakan sesuatu tentang mereka atau perusahaan mereka?
- Apakah anda mengambil langkah-langkah yang msuk akal untuk melindungi rahasia pelanggan dan integrasi dari sistem komputer pelanggan?

Etika Menggunakan Komputer

Etika komputer adalah sebuah frase yang sering digunakan namun sulit untuk didefinisikan. Untuk menanamkan kebiasaan komputer yang sesuai, etika harus dijadikan kebijakan organisasi etis. Sejumlah organisasi mengalamatkan isu mengenai etika komputer dan telah menghasilkan *guideline*etika komputer, kode etik. Berbeda dengan ilmu komputer,yang hanya eksis pada abad ini, ilmu dan disiplin lainnya telah memiliki waktu yang lebih panjang untuk mengembangkan standard dan prinsip etis yang menginformasikan perkembangan baru.

Persoalan etis khusus komputer muncul dari karakteristik unik komputer dan peran yang mereka mainkan. Komputer sekarang adalah media penyimpanan modern, aset yang dapat dinegoisasikan ,sebagai tambahan bentuk baru aset dalam diri mereka sendiri. Komputer juga melayani sebagai instrument kegiatan ,sehingga tingkatan dimana provider layanan komputer dan user harus bertanggung jawab bagi integritas output komputer menjadi sebuah persoalan. Lebih jauh lagi kemajuan teknologi seperti Artificial intelligence, mengancam untuk menggantikan manusia dalam kinerja beberapa tugas, mengambil proporsi menakut-nakuti. Kebutuhan terhadap profesionalisme dalam wilayah penyedia layanan (service provider) dalam industri komputer ,sebagaimana bagian sistem personal yang mendukung dan memelihara komputer teknologi, benar-benar diakui.

Kode etik adalah konsekuensi alamiah realisasi komitmen Mewarisi keamanan penggunaan teknologi komputer baik sektor publik dan swasta. Ada kebutuhan paralel bagi profesionalisme pada bagian pengguna sistem komputer, dalam terminologi tanggung jawab mereka untuk beroperasi secara legal dengan respek penuh dalam urutan yang benar. User harus dibuat sadar terhadap resiko operasi ketika sistem sedang digunakan atau diinstal ;mereka memiliki tanggung

jawab untuk mengidentifikasi dan mengejar penyelewengan dalam hal keamanan. Ini akan memberikan sikap etis dalam komunitas pengguna.

Pendidikan dapat memainkan peran yang sangat penting dalam pengembangan standar etika dalam hal layanan komputer dan komunitas user. Pembukaan komputer terjadi pada masa awal dibanyak negara paling sering di level sekolah dasar. Ini menghadirkan kesempatan yang bernilai untuk mengenalkan standar etika yang dapat. Silahkan menggandakan bahan ajar ini, selama tetap mencantumkan nota hak cipta ini". Diperluas sebagai mana anak-anak maju melalui sekolah dan memasuki tekanan kerja. Universitas dan lembaga belajar yang lebih tinggi harus memasukkan etika komputer ke dalam kurikulum sejak persoalan etika muncul dan memiliki konsekuensi diseluruh area lingkungan komputer. Pada tahun 1992, pengakuan bahwa dengan peningkatan masyarakat kebergantungan terhadap standar teknologi komputer menjamin ketersediaan dan Operasi yang dimaksudkan sistem yang dibutuhkan, OECD menggunakan garis pedoman bagi keamanan sistem informasi. Seiring peningkatan ketergantungan hasil terhadap peningkatan sifat mudah kena serang, standar untuk melindungi keamanan sistem informasi sama pentingnya. Prinsip-prinsip yang OECD promosikan memiliki aplikasi yang lebih luas bahwa keamanan sistem informasi; benar-benar relevan terhadap teknologi komputer secara umum. Yang paling penting diantara prinsip-prinsip ini adalah penyataan bahwa etika yang mengakui kebenaran dan legitimasi kepentingan yang lain dalam menggunakan dan pengembangan teknologi baru promosi etika komputer positif membutuhkan inisiatif dari semua sektor sosial pada level lokal, nasional dan internasional. Keuntungan pokok, bagaimanapun, akan dirasakan komunitas global.

Sepuluh Perintah Etika Komputer

Pada tahun 1992, koalisi etika komputer yang tergabung dalam lembaga etika komputer (CEI) memfokuskan pada kemajuan teknologi informasi, etik dan perusahaan serta kebijakan publik. CEI mengalamatkannya pada kebijakan organisasi, publik, indutrial, dan akademis. Lembaga ini memperhatikan perlunya isu mengenai etika berkaitan degan kemajuan teknologi informasi dalam masyarakat dan telah menciptakan sepuluh perintah etika komputer:

1. Tidak menggunakan komputer untuk merugikan orang lain

2. Tidak mengganggu pekerjaan komputer orang lain
3. Tidak memata-matai file komputer orang lain
4. Tidak menggunakan komputer untuk mencuri
5. Tidak menggunakan komputer untuk bersaksi palsu
6. Tidak menyalin atau menggunakan kepemilikian perangkat lunak dimana anda belum membayarnya
7. Tidak menggunakan sumber daya komputer orang lain tanpa otorisasi atau kompensasi yang sesuai
8. Tidak mengambil untuk diri sendiri karya intelektual orang lain
9. Harus memikirkan tentang konsekuensi sosial program yang anda tulis bagi sistem yang anda desain
10. Harus menggunakan komputer yang menjamin pertimbangan dan bagi sesama manusia.

C. SOAL LATIHAN/TUGAS

1. Apa yang dimaksud system informasi?
2. Jelaskan macam-macam ancaman terhadap system informasi?
3. Bagaimana cara mengamankan system informasi?

D. DAFTAR PUSTAKA

Bagio Budiarjo. *Komputer dan Masyarakat*. PT.Elex Media Komputindo, Jakarta