Cara penanganan agar etika diperhatikan oleh setiap pengguna

Penanganan agar etika diperhatikan oleh setiap pengguna adalah karena etika terkait dengan bidang hukum, maka pengguna harus mengetahui undang–undang yang membahas tentang HAKI (hak atas kekayaan intelektual) dan pasal–pasal yang membahas hal tersebut.Hukum Hak Cipta bertujuan melindungi hak pembuat dalam mendistribusikan , menjual , atau membuat turunan dari karya tersebut. Perlindungan yang di dapatkan oleh pembuat (author) yakniperlindungan terhadap penjiplakan (plagiat) oleh orang lain. Hak cipta sering di asosiasikan sebagai jual beli lisensi, namun distribusi hak cipta tersebut tidak hanya dalam konteks jual beli, sebab bisa saja seorang pembuat karya membuat pernyataan bahwa hasil karyanya bebas dipakai dan di distribusikan.

Antisipasi Pelanggaran Hak Cipta

Guna mengantisipasi terhadap pelanggaran hak cipta, maka dapat dilakukan langkah langkah antara lain:

1. Membuat ketentuan layanan (*Terms of Condition* atau *Terms of Service*) mengenai pembatasan tanggung jawab.
2. Mengembangkan prosedur pemblokiran dan pemutusan layanan yang tepat.

Menghargai Karya Orang Lain antara lain dengan cara:

1. Tidak memakai program komputer bajakan
2. Membuat salinan cadangan program komputer orisinil semata-mata untuk dipakai sendiri
3. Menyebutkan sumber secara lengkap dan jelas ketika melakukan pengutipan informasi
4. Melakukan Pengutipan Sesuai Ketentuan

13.10 Isu-isu Pokok dalam Etika Teknologi Informasi

1. **Cyber Crime**

Merupakan kejahatan yang dilakukan seseorang atau kelompok orang dengan menggunakan komputer sebagai basis teknologinya.

- **Hacker** : seseorang yang mengakses komputer / jaringan secara ilegal
- **Cracker** : seseorang yang mengakses komputer / jaringan secara ilegal dan memiliki niat buruk
- **Script Kiddie** : serupa dengan cracker tetapi tidak memilki keahlian teknis
- **CyberTerrorist** : seseorang yang menggunakan jaringan / internet untuk merusak dan menghancurkan komputer / jaringan tersebut untuk alasan politis.

Contoh pekerjaan yang biasa dihasilkan dari para cyber crime ini adalah berkenaan dengan keamanan, yaitu:

Malware, bagiannya yaitu:

a. **Virus** : program yang bertujuan untuk mengubah cara bekerja komputer tanpa seizin pengguna
b. **Worm** : program-program yang menggandakan dirinya secara berulang-ulang di komputer sehingga menghabiskan sumber daya
c. **Trojan** : program / sesuatu yang menyerupai program yang bersembunyi di dalam program komputer kita.

2. **Denial Of Service Attack**

Merupakan serangan yang bertujuan untuk akses komputer pada layanan web atau email. Pelaku akan mengirimkan data yang tak bermanfaat secara berulang-ulang sehingga jaringan akan memblok pengunjung lainnya.

a. **BackDoor** : program yang memungkinkan pengguna tak terotorisasi bisa masuk ke komputer tertentu.
b. **Spoofing** : teknik untuk memalsukan alamat IP komputer sehingga dipercaya oleh jaringan.

3. **Penggunaan Tak Terotorisasi**

Merupakan penggunaan komputer atau data-data di dalamnya untuk aktivitas illegal atau tanpa persetujuan

4. **Phishing / pharming**

Merupakan trik yang dilakukan pelaku kejahatan untuk mendapatkan informasi rahasia.Jika phishing menggunakan email, maka pharming langsung menuju ke web tertentu.

a. Spam
   Email yang tidak diinginkan yang dikirim ke banyak penerima sekaligus.
b. Spyware
   Program yang terpasang untuk mengirimkan informasi pengguna ke pihak lain.

5. **Cyber Ethic**

Dampak dari semakin berkembangnya internet, yang didalamnya pasti terdapat interaksi antar penggunanya yang bertambah banyak kian hari, maka dibutuhkan adanya etika dalam penggunaan internet tersebut.

6. **Pelanggaran Hak Cipta**

Merupakan masalah tentang pengakuan hak cipta dan kekayaan intelektual, dengan kasus seperti pembajakan, cracking, illegal software. Berdasarkan laporan Bussiness Software Alliance (BSA) dan International

Data Corporation (IDC) dalam Annual Global Software Piracy 2007, dikatakan Indonesia menempati posisi 12 sebagai negara terbesar dengan tingkat pembajakan software.

7. **Tanggung Jawab Profesi TI**

Sebagai tanggung jawab moral, perlu diciptakan ruang bagi komunitas yang akan saling menghormati di dalamnya, Misalnya IPKIN (Ikatan Profesi Komputer & Informatika) semenjak tahun 1974.

Jenis Pelanggaran

a. Hacker

Hacker adalah adalah orang yang mempelajari, menganalisa, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.

Hacker berdasarkan pola pikirnya terdapat 6 jenis :

1. White Hat Hacker
2. Red Hat Hacker
3. Yellow Hat Hacker
4. Black Hat Hacker
5. Green Hat Hacker
6. Blue Hat Hacker
7. Grey Hat Hacker

Solusi Penanggulan serangan hacker adalah mencari kelemahan sistem jaringan atau bug-bug yang ada, karena hacker menyerang dengan memanfaatkan security hole yang ada pada sistem, sehingga ia dapat mengakses secara penuh targetnya. Keamanan juga harus selalu di-update setiap periode waktu karena hacker pasti selalu mencari cara baru untuk dapat menerobos targetnya.

b. Denial of Service Attack

Didalam keamanan computer, Denial of Service Attack (DoS Attack) adalah suatu usaha untuk membuat suatu sumber daya computer yang ada tidak bisa digunakan oleh para pemakai. Tidak bisa digunakan karena penyerang mengirim sebuah paket ke targetnya dengan jumlah yang banyak dan terus berulang sehingga sumber daya targetnya habis.

Denial of Service Attack mempunyai dua format umum :

1. Memaksa computer computer korban untuk mereset atau korban tidak bisa lagi menggunakan perangkat komputernya seperti yang diharapkannya.
2. Menghalangi media komunikasi antara para pemakai dan korba sehingga mereka tidak bisa lagi berkomunikasi.

Denial of Service Attack ditandai oleh suatu usaha eksplisit dengan penyerang untuk mencegah para pemakai memberi bantuan dari penggunaan jasa tersebut..

Contoh :

1. Mencoba untuk " membanjiri " suatu jaringan, dengan demikian mencegah lalu lintas jaringan yang ada.
2. Berusaha untuk mengganggu koneksi antara dua mesin., dengan demikian mencegah akses kepada suatu servce.
3. Berusaha untuk mencegah individu tertentu dari mengaksessuatu service.
4. Berusaha untuk menggangu service kepada suatu orang atau system spesifik.

Cara terbaik untuk mencegah DOS adalah dengan melakukan pencegahan, caranya adalah dengan :

1. Memasang Firewall
2. Menginstal IDS
3. Memeriksa jaringan secara reguler
4. Membuat tim khusus untuk mencegah dan mengatasi DDOS pada jaringan

c. Pelanggaran Piracy

Piracy adalah pembajakan perangkat lunak (software)
Contoh : pembajakan software aplikasi (Microsoft, lagu MP3,MP4, dll)
Keuntungan : biaya yang harus dikeluarkan user relative murah.
Kerugian : merugikan pemilik hak cipta (royalti) secara moral hal ini merupakan pencurian hak milik orang lain.
Solusi : gunakan software aplikasi open source.
Undang undang yang melindungi HAKI : UU no 19 tahun 2002.
Lima macam bentuk pembajakan perangkat lunak :

1. Memasukan perangkat lunak illegal ke harddisk.
2. Softlifting, pemakaian lisensi melebihi kapasitas
3. Penjualan CDROM illegal
4. Penyewaal perangkat lunak illegal
5. Download illegal

Solusi pencegahannya adalah dengan menghimbau masayarakat untuk menggunakan perangkat lunak yang asli. Mengatur UUD yang jelas tentang pembajakan ini dan hukumannya apabila melanggar.

d. Fraud

Merupakan kejahatan manipulasi informasi dengan tujuan mengeruk keuntungan yang sebesar besarnya. Biasanya kejahatan yang dilakukan adalah memanipulasi informasi keuangan.Sebagai contoh adanya situs lelang fiktif. Melibatkan berbagai macam aktifitas yang berkaitan dengan kartu kredit.

e. **Gambling**

Perjudian tidak hanya dilakukan secara konfensional, akan tetapi perjudian sudah marak didunia cyber yang berskala global. Dan kegiatan ini dapat diputar kembali dinegara yang merupakan “tax heaven” seperti cyman islands yang merupakan surga bagi money laundering.

13.11 Peran Etika Dalam Ilmu Pengetahuan Dan Teknologi

Perkembangan Ilmu Pengetahuan dan Teknologi berlansung sangat cepat. Dengan pekembangantersebut diharapkan akan dapat mempertahankan dan meningkatkan taraf hidup manusia.Untuk menjadi manusia secara utuh. Maka tidak cukup dengan mengandalkan IlmuPengetahuan dan Teknologi, manusia juga harus menghayati secara mendalam kode etik ilmu,teknologi dan kehidupan. Apabila manusia sudah jauh dari nalai-nilai, maka kehidupan ini akanterasa kering dan hampa. Oleh karena ilmu dan teknologi yang dikembangkan oleh manusiaharus tidak mengabaikan nilai-nilai kehidupan dan keluhuran.Penilaian seorang ilmuwan yang mungkin salah dan menyimpang dari norma, seyokyanya dapatdigantikan oleh suatu etika yang dapat menjamin adanya suatu tanggung jawab bersama, yaknipihak pemerintah, masyarakat serta ilmuwan itu sendiri.

13.12 Contoh Kasus Dalam Etika Komputer Dan Teknologi

Perkembangan dunia teknologi informasi saat ini merupakan suatu kemajuan yang sangat baik dalam hal teknologi informasi. Kita dapat memperoleh berbagai informasi dengan mudah, tanpa harus bersusah payah dalam memperoleh informasi tersebut. Dengan kemudahan-kemudahan yang didapatkan dalam dunia teknologi informasi kita dapat memperoleh hal positif maupun negatif dari perkembangan tersebut. Namun hal negatif pun banyak kita rasakan, mulai dari penipuan melalui internet, Cyber Crime, Spywere, pembobolan jaringan yang dapat merugikan pihak lain, bahkan penipuan yang memanfaatkan media jejaring sosial dalam dunia maya.Dengan kemudahan yang disediakan di dunia teknologi informasi inilah yang menimbulkan berbagai tindak kejahatan di dalam dunia maya. Kemudahan dalam membuat situs website baik yang berbayar atau yang geratis, maupun karna dilatar

belakangi oleh kebutuhan finansial dari sang pelaku atau bahkan ada yang menjadikan kejahatan didunia maya menjadi sebuah profesi yang menjanjikan.

Pembahasan mengenai beberapa hal kejahatan atau pelanggaran etika dalam dunia maya atau teknologi informasi, yaitu :

1. Data Forgery

Dunia perbankan melalui Internet (e-banking) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang hacker dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan Internet banking Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain www.klik-bca.com, www.kilkbca.com, www.clikbca.com,
www.klickca.com. Dan www.klikbac.com. Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (login form) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (user id) dan nomor identitas personal (PIN) dapat di ketahuinya.

2. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

3. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya

4. kasus pelanggaran etika dalam dunia maya dan teknologi informasi

Pada tahun 1983, pertama kalinya FBI menangkap kelompok kriminal komputer The 414s(414 merupakan kode area lokal mereka) yang berbasis di Milwaukee AS. Kelompok yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer-komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Salah

seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

5. Pelanggaran Hak Cipta di Internet

Seseorang dengan tanpa izin membuat situs penyayi-penyayi terkenal yang berisikan lagu-lagu dan liriknya, foto dan cover album dari penyayi-penyayi tersebut. Contoh : Bulan Mei tahun 1997, Group Musik asal Inggris, Oasis, menuntut ratusan situs internet yang tidak resmi yang telah memuat foto-foto, lagu-lagu beserta lirik dan video klipnya.

Alasannya:

Grup musik tersebut yang dapat menimbulkan peluang terjadinya pembuatan poster atau CD yang dilakukan pihak lain tanpa izin.

Solusi :

Pelanggaran hak cipta secara online juga mencakup pembajakan DMCA, layanan internet perlindungan hak cipta yang sedang berlangsung, layanan berlangganan perlindungan hak cipta secara online, anti-pembajakan perlindungan dan pelayanan pemberitahuan pelanggaran hak cipta dan pelanggaran hak cipta situs.

6.Pelanggaran Piracy

Piracy adalah pembajakan perangkat lunak (software). Apple iPhone berada di tengah kontroversi yang cukup besar awal tahun ini, di mana ketika para peneliti mengungkapkan adanya bug di sistem operasi perangkat iOS yang menyimpan data lokasi GPS dalam folder yang terlindungi. Informasi tersebut memungkinkan aparat penegak hukum, detektif swasta dan pihak lainnya menggunakan iPhone untuk melacak pengguna perangkat di setiap tempat di mana mereka berada, karena setiap saat iPhone melakukan ping ke sebuah menara seluler untuk GPS koordinat lalu disimpan pada perangkatnya. Ketika berita ini keluar, banyak protes yang mencuat dari kalangan pemilik smartphone tersebut.

Meskipun pada saat itu banyak pengguna yang protes, sebuah survei baru dari AdaptiveMobile menemukan bahwa 65 persen dari pemilik iPhone sebetulnya tidak menyadari fakta bahwa aplikasi yang mereka download ke perangkat mereka berpotensi melanggar privasi mereka. Survei AdaptiveMobile global ini dilakukan terhadap 1.024 pengguna iPhone.

Aplikasi berbahaya pada smartphone memang bukan kasus yang benar-benar baru. Pada sistem operasi Google Android pun pernah terdapat virus dan aplikasi yang mampu mencuri data.Untuk iPhone sendiri, Proses pemeriksaan perusahaan Apple cukup ketat sebelum aplikasi disetujui untuk dijual di App Store, namun salah satu ahli keamanan mencatat bahwa masih

banyak kemungkinan pengeksploitasian lubang keamanan di iOS yang berpotensi adanya pembajakan iPhone.

Sementara AdaptiveMobile menemukan bahwa sebagian besar pengguna iPhone tidak menyadari ancaman keamanan potensial pada perangkat mereka, ia juga menemukan bahwa 7 dari 10 pengguna cenderung menganggap pelanggaran privasi yang notabene merupakan sebuah kejahatan.

Dari sudut pandang AdaptiveMobile, kurangnya kesadaran beberapa pengguna iPhone membuat informasi mereka dapat dicuri bahkan membuat proses pencurian informasi tersebut lebih mudah. Kurangnya pengetahuan pengguna dapat menyebabkan cybercrime.

Alasan menggunakan pembajakan:

1. Lebih murah ketimbang membeli lisensi asli
2. Format digital sehingga memudahkan untuk disalin kemedia lain
3. Manusia cenderung mencoba hal baru
4. Undang undang hak cipta belum dilaksanakan dengan tegas
5. Kurangnya kesadaran dari masyarakat untuk menghargai ciptaan orang lain.

Solusi : gunakan software aplikasi open source.
Undang undang yang melindungi HAKI : UU no 19 tahun 2002.

Soal

1. Apa potensi kerugian yang disebabkan pemanfaatan teknologi informasi ?
2. sebutkan pelanggaran yang sering terjadi di dalam pemanfaatan TI ?