

PERTEMUAN 12

PRIVACY DAN KEJAHATAN KOMPUTER

1. Kejahatan Komputer

Kejahatan komputer adalah segala pelanggaran hukum pidana yang melibatkan pengetahuan teknologi komputer untuk persiapan, penyelidikan, dan penuntutan mereka. Dengan penggunaan dan penyalahgunaan komputer ke berbagai ranah baru, pengertian kejahatan komputerpun berubah pengertiannya. Dengan adanya aplikasi komputer yang digunakan tidak hanya di komputer. Kejahatan komputerpun meluas ke berbagai bidang contohnya telekomunikasi, baik digunakan langsung maupun tidak langsung.

Yang sangat sesuai untuk mendefinisikan kejahatan komputer pada saat sekarang ini adalah segala tindakan ilegal yang menggunakan pengetahuan komputer yang ditujukan untuk perbuatan kejahatan atau melanggar hukum. Contoh dari kejahatan komputer antara lain pencurian hardware dan software, manipulasi data, mengakses sistem tanpa izin atau ilegal dan masih banyak lagi.

Kejahatan komputer terus berkembang sejalan dengan perkembangan teknologi, salah satunya adalah penyebaran virus komputer. Contoh beberapa virus komputer yaitu :

A. Worm

Adalah virus yang memiliki sifat seperti parasite karena dapat memperbanyak dirinya sendiri yang jika dibiarkan terus menerus akan membuat penyimpanan pada komputer penuh, yang kemudian menyebabkan sistem pada komputer menjadi mudah rapuh. Tidak hanya memperbanyak dirinya, Worm juga dapat membuat file yang tidak berguna pada suatu komputer yang terjangkit. Oleh karena itu tidak heran jika hardisk pada komputer yang terjangkit menjadi cepat penuh. Virus ini memiliki penyebaran lokasi sama seperti Trojan, yaitu ke tempat yang terhubung dengan internet seperti e-mail.



Gambar 12.1 Ilstrasi virus worm

B. Trojan

Virus inipun mampu untuk mencuri dan mengendalikan data yang ada di dalam komputer. Biasanya virus ini menyebar ke komputer yang terhubung dengan internet, seperti melalui e-mail ataupun data pribadi lainnya seperti yang tidak dikunci dengan password. Pada awalnya Trojan tidak dimasukan ke dalam kategori virus. Namun karena sifatnya sangat mengganggu, akhirnya Trojan dimasukan ke dalam golongan virus komputer. Beberapa anti virus untuk menghindari dari virus ini contohnya Trojan Hunter dan Trojan Remover. Tidak berarti bahwa dengan menggunakan anti virus ini maka komputer anda akan terhindar dari Trojan, tapi paling tidak dapat mengurangi kemungkinannya komputer terjangkit Trojan. Contoh Trojan yang dikirim melalui email baru-baru ini salah satunya adalah e-mail yang berisi file Exel yang seolah-olah atau diduga dikirim oleh WHO padahal ini adalah Trojan-Downloader yang diam-diam akan menginstal file berbahaya lainnya.



Gambar 12.2 Trojan

C. Multipartite Virus

Merupakan jenis virus komputer yang bersembunyi pada RAM komputer. Virus ini akan menginfeksi sistem operasi tertentu dan jika tidak segera ditangani akan menyebar dan menginfeksi hardisk. Virus ini sangat berbahaya bagi RAM karena menyerang secara cepat dan dapat memformat hardisk dan menyebabkan beberapa aplikasi tidak dapat terbuka.



Gambar 12.3 Ilustrasi virus Multipartite

k. FAT Virus

FAT virus atau File Allocation Table virus, yang sesuai dengan namanya adalah virus yang mampu merusak file-file tertentu. Biasanya virus ini bersembunyi pada lokasi penyimpanan pribadi. Virus ini mempunyai cara kerja yang unik, seperti menyembunyikan file-file penting yang seolah-olah file tersebut sudah terhapus atau hilang karena sulit atau bahkan tidak dapat ditemukan.

l. Virus Backdoor

Virus ini biasanya memiliki bentuk yang serupa dengan file yang baik-baik saja. Virus ini lebih menyerang pada mekanisme yang bisa dipakai atau dapat mengakses sistem, jaringan atau aplikasi. Contohnya seperti meminta proses login ataupun autentifikasi.

m. Web Scripting Virus

Virus ini sama seperti Trojan yang awalnya tidak dimasukan dalam kategori virus, namun Web Scripting Virus ini adalah sebuah kode program dimana digunakan untuk menjalankan konten yang ada di dalam suatu website. Sifat dari virus ini dianggap sangat mengganggu program pada komputer yang oleh sebab itu dimasukan ke dalam virus komputer. Salah satu cara mengatasi virus ini adalah dengan membersihkan komputer secara rutin dengan menggunakan anti virus.

n. Memory Resident Virus

Ini adalah virus yang sengaja diciptakan yang ditujukan untuk menginfeksi dan merusak RAM. Jika suatu komputer sudah terjangkit oleh virus ini maka beberapa program pada komputer akan mulai terganggu dan menjadi lambat. Virus ini akan aktif dengan otomatis saat komputer dinyalakan.

o. Companion Virus

Virus ini bertujuan untuk mengganggu data pribadi pemilik komputer. Virus ini biasanya bersembunyi pada hardsik, sehingga cukup sulit untuk ditemukan atau sulit terdeteksi. Contoh dari adanya virus ini pada komputer adalah missal, suatu file yang berformat .jpg akan berubah menjadi .Apk. Karena perubahan format pada file ini maka akan menyebabkan sulitnya menemukan file yang sebenarnya.

p. Directory Virus

Virus ini menyerang dan menjangkit file yang memiliki format exe, yang cara kerjanya dengan membuat file dengan format tersebut menjadi error saat digunakan atau bahkan hilang tanpa alasan yang jelas. Virus ini akan aktif dan menginfeksi secara otomatis ketika suatu program dijalankan.

q. Macro Virus

Virus ini sering kali dibuat dengan sengaja dengan menggunakan bahasa pemrograman suatu aplikasi, bukan dari suatu bahasa pemrograman sistem operasi. Contohnya macro yang ada pada Microsoft Word. Virus ini biasanya menyerang file yang mempunyai format .pps, .xsl, .dcom, ataupun file yang memiliki sifat macro lainnya. Virus ini juga biasanya datang melalui e-mail. Salah satu cara menghindari file ini adalah jangan membuka link yang dikirim melalui email yang tidak jelas asalnya.



Gambar 12.4 Ilustras macro yang ada pada Microsoft Word

r. Spam/Spamming

Spam adalah tindakan mengirimkan iklan atau pesan melalui email atau pesan elektronik lainnya, tanpa izin atau tidak dikehendaki. Contoh dari spamming antara lain mengirimkan

pesan yang berisi menginformasikan bahwa memenangkan hadiah tertentu. Jika mendapat pesan seperti ini baiknya diabaikan saja, karena dikhawatirkan jika kita membalasnya maka akan terjerumus ke penipuan yang dilakukan oleh pelaku spamming.



Gambar 12.5 Spam

s. Carding

Kejahatan komputer dengan cara carding bisa juga dikategorikan sebagai pencurian yang bersifat digital. Carding adalah aktifitas belanja secara ilegal dengan menggunakan nomor atau identitas kartu kredit orang lain. Pelaku carding disebut carder. Indonesia berada di posisi kedua dengan kejahatan carding terbanyak di dunia, posisi pertama ditempati oleh Ukraina.



Gambar 12.6 Carding

t. Phishing

Phishing adalah kegiatan menipu pengguna internet sehingga mereka dengan tidak sadar memberikan informasi penting seperti data diri, *password* dan lainnya. Kejahatan phishing ini biasanya ditujukan kepada pengguna *electronic banking* (*internet banking*).

u. Hacking

Hacking adalah kegiatan mengakses sistem milik pihak lain melalui sistem operasional lain yang dilakukan oleh hacker. Hacking bisa digunakan untuk tujuan baik ataupun tujuan buruk

yaitu kejahatan. Tujuan baik dari hacking ini adalah mengamati keamanan suatu program dan apabila ditemukan celah atau bug pada suatu sistem yang dimasuki maka akan melaporkannya kepada pemilik program. Kegiatan hacking yang bertujuan buruk atau kejahatan adalah seperti mengacak-acak atau merusak suatu program atau sistem.

v. Cracking

Jika hacking bisa bertujuan baik atau jahat, maka cracking bisa dikatakan adalah lebih menjurus tindakan kejahatan. Kegiatan cracking biasanya merusak bahkan mengambil data atau informasi penting. Cracking cenderung meretas suatu sistem atau program hanya untuk kesenangan tersendiri.

2. Faktor Meningkatnya Kejahatan Komputer

Beberapa faktor yang menyebabkan peningkatan dalam kejahatan komputer, antara lain :

a. Meningkatnya penggunaan internet

Internet adalah faktor utama dalam terjadinya kejahatan komputer. Hal ini dapat terjadi karena banyaknya komputer yang tersambung dengan internet. Saat ini masyarakat banyak menggunakan internet pada komputer mereka tanpa memedulikan keamanan pada komputer.

b. Transisi dari single vendor ke multi vendor

Maksudnya adalah saat ini seorang network security harus menguasai tidak hanya satu jenis aplikasi tapi harus menguasai banyak aplikasi dari berbagai vendor. Dengan kata lain kita kekurangan sumber daya yang mengerti tentang network security.

c. Mudahnya mendapatkan software

Saat ini software komputer mudah untuk mendapatkannya, bahkan bisa di download menggunakan internet. Software yang dapat di downloadpun beragam, baik yang bertujuan positif ataupun negatif.

d. Meningkatnya kemampuan pengguna (*user*)

Dengan mudahnya mendapatkan software, para pengguna dapat mempelajari suatu program dengan mudah dan memiliki keinginan untuk mencobanya. Para pengguna umumnya melakukan tindak kejahatan komputer ini hanya bertujuan untuk menguji kemampuan dan kepuasan diri.

e. Penegakan hukum yang lemah

Di Indonesia kita memiliki Undang-Undang ITE namun pada implementasinya masih belum maksimal dan sering kali terlalu dipaksakan.

3. Keamanan Komputer

Keamanan komputer adalah sangat penting untuk diperhatikan dalam mengamankan data-data penting dan informasi pribadi untuk menghindari adanya pencurian informasi.

Beberapa hal yang dapat dilakukan untuk meningkatkan keamanan komputer adalah :

- a. Gunakan password pada komputer dan jangan informasikan kepada sembarang orang.
- b. Rubah password pada komputer, atau akun email dan semacamnya secara berkala.
- c. Gunakan antivirus untuk menangkal masuknya virus dan sejenisnya agar tidak masuk ke dalam komputer.
- d. Jangan mudah memberikan username atau password akun anda saat anda masuk ke suatu website yang terasa janggal.
- e. Buatlah backup data secara berkala.

4. Kejahatan Komputer di Masyarakat

Masyarakat tidak hanya menjadi korban dari tindak kejahatan komputer, tetapi banyak kasus masyarakat juga menjadi salah satu pelakunya. Jika pada posisi masyarakat menjadi korban dimana mereka dirugikan baik dengan kehilangan data-data, ataupun material seperti penipuan yang mengatasnamakan undian dan harus membayar sejumlah uang sebagai biaya

administrasi dan sejenisnya. Kasus-kasus yang sering terjadi dimana masyarakat sebagai pelaku antara lain :

- a. Penyebaran informasi yang tidak benar.
- b. Pelanggaran hak cipta seperti menyebarkan buku atau lagu secara online yang bisa diunduh secara bebas tanpa izin dari pemilik hak cipta.
- c. Melakukan plagiat pada hasil karya ilmiah orang lain yang diunduh ke akun pribadi dan mengatasnamakan karya tersebut sebagai hasil karyanya.
- d. Pemalsuan akun di sosial media, dan masih banyak lagi.

Kejahatan komputer dilatarbelakangi dengan bermacam-macam motif dan cara yang bisa terjadi. Motif dari kejahatan komputer dibagi menjadi :

- a. Motif intelektual

Adalah kejahatan yang dilakukan untuk tujuan kepuasan pribadi untuk menunjukkan bahwa dirinya mampu untuk merekayasa, mengimplementasikan bidang teknologi informasi.

- b. Motif ekonomi, politik, dan ekonomi

Adalah sebuah kejahatan yang dilakukan untuk mendapatkan keuntungan baik secara pribadi atau pada golongan tertentu yang berdampak pada kerugian pada pihak lain, baik secara ekonomi maupun politik.

5. Privacy

Privacy adalah hak seseorang untuk bebas dari intrupsi oleh orang lain ke dalam urusan pribadinya atau “hak untuk dibiarkan sendiri”. Pengertian privacy pada setiap orang dapat berbeda dengan melihat hubungan antar tiap orang. Dan ada beberapa keadaan dimana hukum suatu negara membuat adanya batasan privacy. Privacy dibagi menjadi 2, yaitu:

a. Privacy fisik

Hak seseorang untuk melarang orang lain yang tidak diinginkan mengenai waktu, ruang dan property milik pribadi.

b. Privacy informasi

Hak seseorang untuk menentukan kapan, bagaimana, dan apa saja informasi yang boleh diberikan kepada pihak lain. Sebuah informasi yang bersifat pribadi (privacy) baiknya hanya dapat diakses oleh user yang berkepentingan. Informasi tersebut tidak dapat diakses oleh khalak umum.

Undang-Undang yang mengatur tentang pidana pelanggaran hak privacy yaitu Undang-Undang ITE yang berbunyi “Barang siapa dengan sengaja melawan hukum memanfaatkan teknologi informasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seizin yang bersangkutan, dipidana penjara paling singkat tiga tahun dan paling lama 7 tahun.”

Contoh pelanggaran privacy:

- a. Membajak akun sosial media orang lain.
- b. Menyebarkan data pribadi milik orang lain tanpa seizin pemilik.
- c. Memperjualbelikan data pelanggan dari satu perusahaan ke perusahaan lain.
- d. Pemalsuan identitas pada media sosial yang ditujukan untuk penipuan.

6. Pengadilan Kejahatan di Dunia Maya

Untuk menanggulangi kejahatan komputer yang semakin meningkat, Indonesia mempunyai undang-undang yang mengatur tentang kejahatan komputer yaitu UU ITE. Undang-undang tersebut antara lain Undang-undang No. 19 Tahun 2016 tentang Perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam penerapan UU ITE ini sering disebut dengan pasal karet. Ini terjadi karena istilah yang digunakan merupakan istilah teknis, dimana dalam prakteknya berbeda antara di dunia teknologi dan di dunia nyata.

Peraturan mengenai tindak pidana di dunia maya di Indonesia bisa diartikan sempit maupun luas, sesuai dengan hasil kongres PBB kesepuluh tentang pencegahan kejahatan dan pelanggaran terhadap pelanggaran yang diselenggarakan di Wina tanggal 10-17 April 2000, yaitu:

a. Dalam arti sempit

Setiap kegiatan ilegal yang dilakukan melalui atau menggunakan perangkat elektronik dimana targetnya adalah keamanan sistem komputer dan data yang diproses oleh mereka.

b. Dalam arti yang luas

Setiap kegiatan yang bersifat ilegal yang dilakukan menggunakan, atau terkait dengan sebuah sistem atau jaringan komputer termasuk kejahatan seperti kepemilikan ilegal, menawarkan atau menyebarkan informasi melalui sistem komputer atau jaringan. Sesuai dengan pengertian tersebut di atas maka tindak pidana konvensional dalam KUHP seperti pembunuhan, perdagangan orang dan lainnya dapat dikategorikan tindak pidana kejahatan komputer jika menggunakan sarana elektronik. Contohnya tindak pidana perbankan dan pencucian uang dalam UU No. 8 Tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang.

Dalam UU ITE kejahatan komputer dibagi dalam beberapa kelompok:

a. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu:

1) Distribusi atau penyebaran konten ilegal

- Kesusilaan.
- Perjudian.
- Penghinaan dan atau pencemaran nama baik.
- Pemerasan dan pengancaman.
- Berita bohong dan menyesatkan dan merugikan konsumen.
- Menimbulkan rasa kebencian berdasarkan SARA.

- Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

2) Tindak pidana yang berhubungan dengan gangguan (interfensi), yaitu:

- Gangguan terhadap informasi atau dokumen elektronik.

- Gangguan terhadap sistem elektronik.

3) Tindak pidana memfasilitasi perbuatan yang dilarang.

4) Tindak pidana pemalsuan informasi atau dokumen elektronik.

5) Perbuatan-perbuatan terhadap hukum pidana.

C. SOAL LATIHAN/TUGAS

1. Bagaimana cara meningkatkan keamanan komputer?

- Memperbarui sistem operasi dan perangkat lunak: Pastikan komputer Anda selalu menggunakan versi terbaru dari sistem operasi dan perangkat lunak, termasuk antivirus dan firewall. Pembaruan tersebut sering kali memperbaiki kerentanan keamanan yang telah ditemukan.
- Menggunakan perangkat lunak keamanan yang kuat: Instal dan aktifkan perangkat lunak antivirus, antispyware, dan firewall yang terpercaya. Pastikan perangkat lunak tersebut diperbarui secara teratur agar dapat mengenali dan mengatasi ancaman terbaru.
- Menggunakan kata sandi yang kuat: Gunakan kata sandi yang panjang, kompleks, dan unik untuk setiap akun online yang Anda miliki. Gabungkan huruf besar dan kecil, angka, dan simbol khusus. Hindari menggunakan kata sandi yang mudah ditebak seperti tanggal lahir atau nama depan.
- Mengaktifkan autentikasi dua faktor (2FA): Aktifkan autentikasi dua faktor di akun-akun yang mendukungnya. Ini menambahkan lapisan keamanan tambahan dengan memerlukan verifikasi kedua, seperti kode yang dikirimkan melalui SMS atau aplikasi autentikasi, selain kata sandi.
- Memeriksa email dan lampiran dengan hati-hati: Jangan mengklik tautan atau membuka lampiran dari email yang mencurigakan atau tidak dikenal. Hal ini dapat menghindari penyebaran malware atau phishing.
- Menghindari mengunduh dari sumber yang tidak dipercaya: Jangan mengunduh perangkat lunak atau file dari sumber yang tidak dipercaya. Dapatkan perangkat lunak hanya dari situs resmi atau sumber tepercaya.
- Mengamankan jaringan Wi-Fi: Pastikan jaringan Wi-Fi Anda dilindungi dengan kata sandi yang kuat dan enkripsi yang tepat. Hindari menggunakan kata sandi default pada perangkat jaringan Anda.
- Melakukan pencadangan data secara teratur: Selalu lakukan pencadangan data penting Anda. Jika terjadi serangan atau kehilangan data, Anda masih memiliki salinan yang dapat dipulihkan.
- Memeriksa izin aplikasi: Ketika menginstal aplikasi baru, periksa dengan cermat izin yang diminta oleh aplikasi tersebut. Berikan izin hanya jika diperlukan dan relevan.
- Menjaga kesadaran dan edukasi: Tingkatkan kesadaran tentang ancaman keamanan komputer yang terbaru. Terus belajar dan mengikuti praktik keamanan yang disarankan untuk menjaga keamanan komputer Anda

2. Jelaskan pengertian privacy secara fisik dan informasi!

Privacy secara fisik mengacu pada hak individu untuk menjaga privasi dan kebebasan dari gangguan atau intervensi fisik oleh pihak lain. Ini melibatkan ruang pribadi seseorang, tubuhnya, dan aktivitas sehari-hari yang tidak boleh diintervensi atau diawasi tanpa izin atau kebutuhan yang sah. Privasi fisik melibatkan hak untuk merasa aman dan tidak terganggu di tempat tinggal, di tempat kerja, atau di tempat umum.