INTRODUCTION TO INFORMATION SYSTEMS

WEEK 13 - CYBERCRIME AND INFORMATION SYSTEM SECURITY

LECTURER : RAMBU YETTI KALAWAY

PENGANTAR

Cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*, penipuan identitas, pornografi anak, dll

CYBERCRIME

Cybercrime atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (Moore, 2005). Komputer mungkin telah digunakan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.

Cybercrime menurut Halder dan Jaishankar (2011) dapat didefinisikan sebagai pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang *Chat, email, notice boards* dan kelompok) dan telepon genggam

CYBERCRIME

Cybercrime dapat mengancam seseorang, keamanan negara atau kesehatan finansial.

Isu seputar jenis kejahatan ini telah menjadi sangat populer, terutama seputar *hacking*, pelanggaran hak cipta, penyadapan yang tidak beralasan dan pornografi.

Ada pula masalah privasi pada saat informasi rahasia dicegat atau diungkapkan, secara sah atau tidak sah.

CYBERCRIME

Menurut Arief (2006) kejahatan cyber merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi.

Beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai " kejahatan dunia maya" (*cyberspace/virtual-space offence*), dimensi baru dari "hi-tech crime", dimensi baru dari "transnational crime", dan dimensi baru dari "white collar crime".

CYBERCRIME

Secara hukum di Indonesia pun telah memiliki undang- undang khusus menyangkut kejahatan dunia maya, yaitu undang ITE tahun 2008, yang membahas tentang tata cara, batasan penggunaan computer dan sangsi yang akan diberikan jika terdapat pelanggaran.

Misalnya perbuatan *illegal access* atau melakukan akses secara tidak sah perbuatan ini sudah diatur dalam pasal 30 undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik disebutkan, bahwa: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain ayat (1)) dengan cara apapun, (ayat (2)) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat (3)) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman

JENIS – JENIS CYBERCRIME

Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*) menurut Sutanto (2004) motif dan penindakan *cybercrime* terdiri dari dua jenis, yaitu:

JENIS – JENIS CYBERCRIME

a. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas

Contoh-contoh dari aktivitas cybercrime jenis pertama ini adalah pembajakan (copyright atau hak cipta intelektual, dan lain-lain); pornografi; pemalsuan dan pencurian kartu kredit (carding); penipuan lewat e-mail; penipuan dan pembobolan rekening bank; perjudian on line; terorisme; situs sesat; materi-materi internet yang berkaitan dengan sara (seperti penyebaran kebencian etnik dan ras atau agama); transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain

JENIS – JENIS CYBERCRIME

b. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran

Cybercrime jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak pidana, melainkan menjadikannya sebagai sasaran.

Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu sistem secara ilegal (hacking), perusakan situs internet dan server data (cracking), serta defecting

JENIS – JENIS CYBERCRIME

Menurut Haris (2001), cybercrime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

a. Unauthorized access (dengan maksud untuk memfasilitasi kejahatan);
b. Unauthorized alteration or destruction of data;
c. Mengganggu/merusak operasi komputer

KUALIFIKASI CYBERCRIME

Kualifikasi kejahatan dunia maya menurut Convention on Cybercrime 2001 di Budapest,Hongaria, yaitu:

a. Illegal interception: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diamdiam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.

b. Data interference: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.

KUALIFIKASI CYBERCRIME

c. System interference: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.

d. Misuse of devices: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code).

KUALIFIKASI CYBERCRIME

e. Computer related forgery: pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)

f. Computer related fraud: penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain);

KUALIFIKASI CYBERCRIME

g. Content-related offences: delik-delik yang berhubungan dengan pornografi anak (child pornography);

h. Offences related to infringements of copyright and related rights: delik-delik yang terkait dengan pelanggaran hak cipta.

KLASIFIKASI CYBERCRIME

Penipuan dan kejahatan finansial

Penipuan dengan menggunakan komputer adalah salah representasi fakta yang tidak jujur yang dimaksudkan untuk membiarkan orang lain melakukan sesuatu yang menyebabkan kerugian.

KLASIFIKASI CYBERCRIME

Kecurangan tersebut dilakukan dengan cara:

- Mengubah dengan cara yang tidak sah. Ini memerlukan sedikit keahlian teknis dan merupakan bentuk pencurian umum oleh seorang karyawan yang mengubah data atau memasukkan data palsu atau dengan memasukkan instruksi yang tidak sah atau menggunakan proses yang tidak sah.
- Mengubah, menghancurkan atau mencuri *output*, biasanya untuk menyembunyikan transaksi yang tidak sah. Ini sulit dideteksi;
- Mengubah atau menghapus data yang tersimpan.

KLASIFIKASI CYBERCRIME

Bentuk kecurangan lainnya dapat difasilitasi dengan menggunakan sistem komputer, termasuk penipuan bank, *carding*, pencurian identitas, pemerasan dan pencurian informasi rahasia.

Berbagai penipuan internet banyak berbasis *phishing* dan *social engineering* yang menjadi sasaran biasanya konsumen dan pelaku bisnis.

KLASIFIKASI CYBERCRIME

Cyberterrorism

Pejabat pemerintah dan spesialis keamanan teknologi informasi telah mendokumentasikan peningkatan yang signifikan dalam masalah Internet dan pemindaian server sejak awal 2001. Namun, ada kekhawatiran yang berkembang di antara lembaga pemerintah FBI dan CIA bahwa intrusi semacam itu adalah bagian dari usaha terorganisir oleh cyberterrorist, dinas intelijen asing atau kelompok lain untuk memetakan potensi celah keamanan dalam sistem kritis

KLASIFIKASI CYBERCRIME

Cyberterrorisme secara umum dapat didefinisikan sebagai tindakan terorisme yang dilakukan melalui penggunaan dunia maya atau sumber daya komputer (Parker,1983).

Sebagai contoh, sebuah propaganda sederhana di Internet akan terjadi serangan bom saat liburan tahun baru bisa dianggap sebagai cyberterrorism. Ada juga kegiatan hacking yang diarahkan pada individu atau keluarga yang diselenggarakan oleh kelompok-kelompok di dalam jaringan, cenderung menimbulkan ketakutan di kalangan orang-orang, mengumpulkan informasi yang relevan untuk menghancurkan kehidupan masyarakat, perampokan, pemerasan, dll

KLASIFIKASI CYBERCRIME

Cyberextortion

Cyberextortion terjadi saat sebuah situs web, server e-mail atau sistem komputer dikenai atau diancam dengan penolakan berulang (Denial of Service / DoS) terhadap layanan atau serangan lainnya oleh hacker jahat.

Para hacker ini menuntut uang sebagai imbalan dengan janji akan menghentikan serangannya dan atau menawarkan "perlindungan".

KLASIFIKASI CYBERCRIME

Saat ini semakin banyak serangan yang dilakukan para pelaku cyberextortion pada situs web perusahaan dan jaringan, melumpuhkan kemampuan / kinerja mereka untuk beroperasi dan menuntut pembayaran untuk memulihkan layanan mereka

Pelaku biasanya menggunakan serangan denial-of-service terdistribusi (distributed denial-of-service / DDoS)

KLASIFIKASI CYBERCRIME

Cyberwarfare

Departemen Pertahanan Amerika Serikat (Department of Defense / DoD) mencatat bahwa dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi geo-strategis.

KLASIFIKASI CYBERCRIME

Komputer sebagai target

Kejahatan ini dilakukan oleh kelompok kriminal terpilih. Tidak seperti kejahatan yang menggunakan komputer sebagai alat, kejahatan ini memerlukan pengetahuan teknis sang pelaku.

Dengan demikian seiring perkembangan teknologi, maka berkembang pula sifat kejahatannya.

KLASIFIKASI CYBERCRIME

Kejahatan ini relatif baru dalam sejarah komputer, yang menjelaskan betapa tidak siapnya masyarakat dan dunia pada umumnya untuk memberantas kejahatan ini. Ada banyak kejahatan dari sifat ini yang dilakukan setiap hari di internet.

Kejahatan yang terutama menargetkan jaringan komputer atau perangkat meliputi:

- Virus komputer.
- Denial-of-service attacks.
- Malware (malicious code)

KLASIFIKASI CYBERCRIME

Komputer sebagai alat

Bila individu merupakan target utama cybercrime, komputer bisa dianggap sebagai alat ketimbang target. Kejahatan ini umumnya kurang melibatkan keahlian teknis.

Kelemahan manusia umumnya dieksploitasi. Kerusakan yang ditangani sebagian besar bersifat psikologis dan tidak berwujud, membuat tindakan hukum terhadap varian ini lebih sulit.

KLASIFIKASI CYBERCRIME

Kejahatan yang menggunakan jaringan komputer lainnya meliputi:

- Penipuan dan pencurian identitas
- Perang informasi.
- Penipuan (phishing)
- Spam
- Pornografi, termasuk pelecehan dan ancaman.

KLASIFIKASI CYBERCRIME

Pengiriman email massal yang tidak diminta untuk tujuan komersial (spam) tidak sah di beberapa wilayah hukum.

Phishing sebagian besar disebarkan melalui email.

Email phishing mungkin berisi tautan ke situs web lain yang terpengaruh oleh malware. Atau, mungkin berisi tautan ke perbankan online palsu atau situs web lain yang digunakan untuk mencuri informasi akun pribadi

KLASIFIKASI CYBERCRIME

Konten tidak senonoh atau menyinggung

Isi situs web dan komunikasi elektronik lainnya mungkin tidak menyenangkan, tidak senonoh atau menyinggung karena berbagai alasan.

Sejauh mana komunikasi ini melanggar hukum sangat bervariasi di antara negara-negara lain.

Ini adalah area sensitif di mana pengadilan dapat terlibat dalam arbitrase antar kelompok dengan keyakinan yang kuat

KLASIFIKASI CYBERCRIME

Salah satu bidang pornografi internet yang telah menjadi sasaran upaya terkuat pada pembatasannya adalah pornografi anak yang ilegal di kebanyakan wilayah hukum di dunia

KLASIFIKASI CYBERCRIME

Pelecehan

Dalam konten ini mungkin menyinggung dengan cara yang tidak spesifik, pelecehan mengarahkan kata-kata kotor, penghinaan atau komentar pada individu tertentu yang memusatkan perhatian pada jenis kelamin, ras, agama, kebangsaan atau orientasi seksual, atau biasa di sebut mengandung unsur SARA. Hal ini sering terjadi di chat room, melalui newsgroup dan dengan mengirim email kebencian ke pihak yang berkepentingan.

Pelecehan di internet juga termasuk balas dendam

KLASIFIKASI CYBERCRIME

Perdagangan narkoba

Pasar gelap digunakan untuk membeli dan menjual obat-obatan terlarang secara online.

Beberapa pedagang narkoba menggunakan alat pesan terenkripsi untuk berkomunikasi dengan pemasok narkoba.

CYBERATTACKS

Keamanan sistem yang memiliki banyak celah dapat menyebabkan seorang hacker memanfaatkan celah keamanan untuk masuk ke dalam sistem, merusak serta mengambil data-data yang tidak seharusnya diketahui olah pihak luar.

Hacker merupakan istilah yang digunakan untuk menggambarkan seorang yang mempelajari, memodifikasi, menerobos masuk ke dalam komputer baik untuk kepentingan sendiri maupun kelompok

CYBERATTACKS

Cyberattacks atau Serangan cyber adalah jenis manuver ofensif yang digunakan oleh negara-negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer dan atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim yang mencuri, mengubah atau menghancurkan target yang ditentukan dengan cara membobol sistem yang rentan

CYBERATTACKS

Ini dapat diberi label sebagai kampanye cyber, cyberwarfare atau cyberterrorism dalam konteks yang berbeda.

Cyberattacks dapat berkisar dari menginstal spyware di PC untuk mencoba menghancurkan infrastruktur seluruh negara.

CYBERATTACKS

Secara rinci, ada sejumlah teknik untuk memanfaatkan serangan cyber dan berbagai cara untuk mengelolanya kepada individu atau perusahaan dalam skala yang lebih luas. Serangan dibagi menjadi dua kategori: serangan sintaksis dan serangan semantik.

CYBERATTACKS

Serangan Sintaksis

Serangan sintaksis sangat mudah hanya menggunakan software berbahaya. Software berbahaya ini termasuk virus, worm, dan trojan horse.

Virus

Virus adalah program replikasi diri yang bisa menempel pada program atau file lain agar bisa bereproduksi. Virus dapat bersembunyi dalam memori sistem komputer dan menempelkan dirinya ke file apa pun yang menurutnya sesuai untuk menjalankan kodenya. Hal ini juga dapat mengubah jejak digitalnya setiap kali bereplikasi sehingga sulit dilacak di komputer

CYBERATTACKS

Worm

Worm tidak memerlukan file atau program lain untuk menyalin dirinya sendiri. Ini adalah program berjalan mandiri.

Worm mereplikasi jaringan dengan menggunakan protokol. Inkarnasi worm terbaru memanfaatkan kerentanan yang diketahui dalam sistem untuk menembus, mengeksekusi kode mereka, dan meniru sistem lain seperti worm Code Red II yang menginfeksi lebih dari 259.000 sistem dalam waktu kurang dari 14 jam

Pada skala yang jauh lebih besar, worm dapat dirancang untuk spionase industri, untuk memantau dan mengumpulkan data dari server lalu mengirimkannya kembali ke penciptanya.

CYBERATTACKS

Trojan Horse

Trojan horse dirancang untuk melakukan tugas yang seakan-akan sah namun juga melakukan aktivitas yang tidak diketahui dan tidak diinginkan. Ini bisa menjadi dasar dari banyaknya penyebaran virus dan worm yang menginstal ke komputer dan juga penyebaran malicious software seperti misalnya keyboard logger dan backdoor software.

Dalam pengertian komersial, Trojan horse dapat tertanam dalam versi trial dari perangkat lunak dan dapat mengumpulkan informasi tambahan tentang target tanpa sepengetahuan orang yg jadi sasarannya

CYBERATTACKS

Serangan semantik

Serangan semantik adalah modifikasi dan penyebaran informasi yang benar dan salah. Informasi yang dimodifikasi bisa saja dilakukan tanpa menggunakan komputer meski peluang baru bisa ditemukan dengan menggunakan komputer. Untuk mengatur seseorang ke arah yang salah atau untuk menutupi jejak , penyebaran informasi yang salah dapat digunakan.

CYBERATTACKS

Berdasarkan tindakan dan motif yang dilakukan oleh seorang yang melakukan cyber crime, menurut Hius, et al. (2014) permasalahan terbagi menjadi lima bagian yaitu :

1. Cyber crime sebagai tindakan kejahatan murni Tindakan kejahatan yang dilakukan secara disengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

CYBERATTACKS

2. Cyber crime sebagai tindakan kejahatan abu-abu.

Tindakan kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

CYBERATTACKS

3. Cyber crime yang menyerang individu

Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi.

Contoh dari tindakan tersebut adalah: pornografi, cyberstalking, dan lain-lain.

CYBERATTACKS

4. Cyber crime yang menyerang hak cipta (hak milik)

Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum ataupun demi materi atau non materi.

CYBERATTACKS

5. Cyber crime yang menyerang pemerintah

Kejahatan yang dilakukan terhadap pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu negara.

MODUS KEJAHATAN CYBERCRIME

Menurut Golose (2006) modus kejahatan cyber crime dibagi ke dalam beberapa bentuk berdasarkan bentuk sesuai modus operasinya seperti berikut:

1. Unauthorized Access to Computer System and Service

Merupakan kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Insiden serangan yang terjadi biasanya dilakukan dengan cara mencuri untuk mendapatkan sebuah informasi penting dan rahasia. Selain itu, ada juga yang melakukan insiden serangan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem.

MODUS KEJAHATAN CYBERCRIME

2. Illegal Contents

Illegal Contents adalah kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

Kejahatan yang biasanya terjadi pada Illegal contents seperti pembuatan suatu berita bohong atau fitnah, dimana berita bohong tersebut dapat menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

MODUS KEJAHATAN CYBERCRIME

3. Data Forgery

Data Forgery adalah kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.

Kejahatan ini biasanya ditujukan pada dokumen-dokumen ecommerce dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

MODUS KEJAHATAN CYBERCRIME

4. Cyber Espionage

Cyber Espionage adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network sistem) pihak sasaran.

Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang terkomputerisasi.

MODUS KEJAHATAN CYBERCRIME

5. Cyber Sabotage and Extortion

Merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

Contoh kejahatan biasanya dengan menyebarkan virus komputer saat korban melakukan browsing di internet.

MODUS KEJAHATAN CYBERCRIME

6. Offense against Intellectual Property

Merupakan kejahatan yang ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet.

Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

MODUS KEJAHATAN CYBERCRIME

7. Infringements of Privacy

Merupakan kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

MODUS KEJAHATAN CYBERCRIME

8. Cracking

Cracking merupakan kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamaanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu merekan mendapatkan akses.

Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identetik dengan perbuatan negatif, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

MODUS KEJAHATAN CYBERCRIME

9. Carding

Carding merupakan kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil

PENYEBAB TERJADINYA CYBERCRIME

Kejahatan yang terjadi pada komputer terus bertambah dan membuat resah.

Terdapat beberapa hal yang menyebabkan makin maraknya kejahatan komputer atau cyber crime, menurut Hius, et al. (2014) seperti berikut:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer.
3. Mudah dilakukan dan sullit untuk melacaknya.
4. Para pelaku umumnya orang yang mempunyai kecerdasan tinggi dan rasa ingin tahu yang besar.

PENANGANAN DAN PENCEGAHAN CYBERCRIME

Insiden serangan yang terjadi dikarenakan cyber crime membuat banyak korban menjadi kesulitan terutama dari sisi keamanan dan juga sisi finansial.

Berdasarkan banyaknya insiden serangan yang disebabkan oleh cyber crime, menurut Arifah (2011) penanganan dan pencegahan dapat di lakukan dengan berbagai cara seperti:

1. *Educate User*

Educate User merupakan penanganan yang dilakukan dengan cara memberikan pengetahuan baru terhadap cyber crime dan dunia internet, bahwa tindakan yang dilakukan oleh pelaku adalah melanggar hukum

PENANGANAN DAN PENCEGAHAN CYBERCRIME

2. Use Hacker's Perspective

Use Hacker's Perspective merupakan penanganan yang dilakukan dengan cara menggunakan pemikiran dari sisi hacker untuk melindungi sistem anda.

3. Patch System

Patch System merupakan penanganan yang dilakukan dengan cara menutup semua lubang kelemahan yang terdapat pada sistem.

PENANGANAN DAN PENCEGAHAN CYBERCRIME

4. Policy

Policy menentukan kebijakan dan aturan yang melindungi sistem anda dari orang-orang yang tidak bertanggung jawab.

5. Firewall

Firewall merupakan sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari berbagai jenis serangan dari komputer luar

6. Anti Virus

Anti Virus merupakan sebuah perangkat lunak yang digunakan untuk mendeteksi, mengamankan, dan menghapus virus kompur seperti: worm, trojan, spyware dan lain-lain dari sistem komputer.

PENANGANAN DAN PENCEGAHAN CYBERCRIME

Beberapa langkah penting yang harus dilakukan dalam pencegahan serangan cyber crime, menurut Arifah (2011) seperti berikut :

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.

PENANGANAN DAN PENCEGAHAN CYBERCRIME

b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara yang berhubungan dengan Cyber crime.

PENANGANAN DAN PENCEGAHAN CYBERCRIME

d. Meningkatkan kesadaran warga negara mengenai masalah cyber crime serta pentingnya mencegah kejahatan tersebut terjadi.

e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cyber crime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.

MEMERANGI KEJAHATAN KOMPUTER

Difusi cybercrime

Difusi luas aktivitas cybercriminal adalah masalah dalam deteksi dan penuntasan kejahatan komputer. Keahlian teknis dan aksesibilitas tidak lagi bertindak sebagai penghalang masuk ke cybercrime.

Memang, hacking jauh lebih rumit daripada beberapa tahun yang lalu, karena komunitas hacker telah menyebarkan pengetahuan mereka melalui Internet. Blog dan komunitas hacker sangat berkontribusi dalam berbagi informasi: seorang hacker pemula bisa mendapatkan keuntungan dari pengetahuan dan saran dari hacker yang lebih senior.

MEMERANGI KEJAHATAN KOMPUTER

Selain pencegahan serangan cyber crime yang dapat dilakukan seperti atas, juga terdapat pencegahan lain, menurut Arifah (2011) seperti berikut:

1. IDCERT (Indonesia Computer Emergency Response Team)

Melaporkan tindakan terkait dengan kasus keamanan di internet kepada tim IDCERT bahwa adanya insiden serangan.

MEMERANGI KEJAHATAN KOMPUTER

2. Membantu negara terhindar dari pelaku kejahatan, seperti teroris, kejahatan terorganisasir, dan operasi penipuan.

3. Membantu negara terhindar dari tempat yang nyaman untuk menyimpan aplikasi atau data hasil kejahatan cyber crime.

4. Meningkatkan kepercayaan pasar karena adanya kepastian hukum yang mampu melindungi kepentingan dalam berusaha

MEMERANGI KEJAHATAN KOMPUTER

5. Memberikan perlindungan terhadap data yang tergolong khusus (classified), rahasia, informasi yang bersifat pribadi, data pengadilan kriminal, dan data publik yang dianggap perlu untuk dilindungi.

6. Melindungi konsumen, membantu penegakan hukum, dan aktivitas intelligen.

7. Meningkatkan keamanan nasional dan mengurangi kerentanan dari serangan dan aksi oleh teroris dan mereka yang berniat jahat.

MEMERANGI KEJAHATAN KOMPUTER

8. Melindungi dunia usaha dari resiko bisnis seperti kehilangan pangsa pasar, rusaknya reputasi, penipuan, tuntutan hukum dari publik, dan kasus perdata maupun pidana.

9. Sebagai sarana untuk menghukum pelaku kejahatan di bidang teknologi informasi.

10. Meningkatkan peluang bagi diakuinya catatan elektronik sebagai alat bukti yang sah di pengadilan dalam kasus kejahatan seperti pencurian, penipuan, pembunuhan, penculikan dan lain – lain, atau kejahatan komputer yang dilakukan menggunakan internet

MEMERANGI KEJAHATAN KOMPUTER

Selanjutnya, hacking lebih murah dari sebelumnya: sebelum era cloud computing, untuk spam atau scam dibutuhkan server yang berdedikasi, ketrampilan dalam manajemen server, konfigurasi jaringan dan pemeliharaan, pengetahuan tentang standar penyedia layanan Internet dan lain-lain.

Cloud computing dapat membantu cybercriminal sebagai cara untuk memanfaatkan serangannya - brute-force password, meningkatkan jangkauan botnet atau memfasilitasi kampanye spamming.

MEMERANGI KEJAHATAN KOMPUTER

Investigasi

Komputer bisa menjadi sumber bukti (forensik digital). Bahkan di mana komputer tidak digunakan secara langsung untuk tujuan kriminal, catatan itu mungkin berisi catatan nilai bagi penyidik kriminal dalam bentuk logfile. Di kebanyakan negara penyedia layanan internet (Internet Service Providers) secara hukum diharuskan untuk menyimpan logfiles mereka untuk jumlah waktu yang telah ditentukan.

Sebagai contoh; Petunjuk Penyimpanan Data Eropa yang luas (berlaku untuk semua negara anggota Uni Eropa) menyatakan bahwa semua lalu lintas E-mail harus dipertahankan minimal selama 12 bulan.

MEMERANGI KEJAHATAN KOMPUTER

Ada banyak cara untuk kejahatan dunia maya bisa terjadi dan penyelidikan cenderung dimulai dengan jejak alamat IP (IP Address), namun itu belum tentu merupakan basis faktual dimana penyidik dapat menyelesaikan sebuah kasus.

Berbagai jenis kejahatan teknologi tinggi mungkin juga mencakup unsur-unsur kejahatan teknologi rendah dan sebaliknya, membuat penyidik dunia maya menjadi bagian tak terpisahkan dari penegakan hukum modern.

Metodologi kerja penyidik cybercrime bersifat dinamis dan terus membaik, baik di unit polisi khusus, maupun dalam kerangka kerjasama internasional

MEMERANGI KEJAHATAN KOMPUTER

Legislasi

Karena undang-undang yang mudah dieksploitasi, penjahat dunia maya menggunakan negara-negara berkembang untuk menghindari deteksi dan penuntutan dari penegak hukum. Di negara berkembang, hukum melawan cybercrime sangat lemah atau terkadang tidak ada.

Undang-undang yang lemah ini memungkinkan penjahat dunia maya menyerang dari perbatasan internasional dan tetap tidak terdeteksi. Bahkan ketika diidentifikasi, penjahat ini menghindari hukuman atau ekstradisi ke negara lain, seperti Amerika Serikat, yang telah mengembangkan undang-undang yang memungkinkan penuntutan

MEMERANGI KEJAHATAN KOMPUTER

Hukuman

Sanksi untuk kejahatan terkait komputer di Negara Bagian New York dapat berkisar dari denda dan masa hukuman penjara yang singkat untuk pelanggaran ringan Kelas A seperti penggunaan komputer yang tidak sah sampai gangguan komputer pada tingkat pertama yang merupakan tindak pidana Kelas C dan dapat dilakukan 3 sampai 15 tahun penjara.

Namun, beberapa hacker telah dipekerjakan sebagai pakar keamanan informasi oleh perusahaan swasta karena pengetahuan mereka tentang kejahatan komputer, sebuah fenomena yang secara teoritis dapat menciptakan insentif yang menyimpang.

MEMERANGI KEJAHATAN KOMPUTER

Kemungkinan penghindaran ini adalah agar pengadilan melarang para hacker yang dipidana menggunakan komputer dan internet dalam bentuk apapun, bahkan setelah mereka dibebaskan dari penjara, meskipun saat komputer dan internet menjadi sangat lebih penting bagi kehidupan sehari-hari, hukuman jenis ini dapat artikan sebagai hukuman lebih keras dan kejam.

Namun, pendekatan lain telah dikembangkan untuk memanage para pelaku kejahatan cyber tanpa larangan total dalam menggunakan komputer atau internet

MEMERANGI KEJAHATAN KOMPUTER

Pendekatan ini melibatkan pembatasan individu terhadap perangkat tertentu yang dapat dilakukan dengan cara pemantauan komputer atau penelusuran komputer oleh petugas percobaan atau pembebasan bersyarat

THANK YOU

R YETTI K

REFERENSI

Arief, Barda Nawawi,2006, Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia. Jakarta: Raja Grafindo Persada.

Arifah, Dista Amalia,2011, Kasus Cybercrime di Indonesia, Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2.

Golose, Petrus Reinhard,2006,Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri, *Buletin Hukum Perbankan dan Kebanksentralan, Vol. 4, No. 2*

Halder, D., & Jaishankar, K.,2011, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global

Haris, Freddy, 2001, Pengantar Menanti Hukum di Cyberspace, Jurnal Hukum dan Teknologi,No. I Vol. I, Jakarta: LKIIT-FHUI, Jakarta

Hius, J. J, Saputra, J, dan Nasution, A.,2014, Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku. Banda Aceh: Prosiding Snikom

Moore, R.,2005, Cyber crime: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing

Parker,D,1983, Fighting Computer Crime, U.S : Charles Scribner's Sons

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, 2004, Cybercrime Motif dan Penindakan, Jakarta: Pensil 324