CONTOH KASUS CYBER CRIME DAN PENYELESAIANNYA
Pengertian Cybercrime

Cybercrime adalah tidak criminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet. Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasasis pada kecanggihan perkembangan teknologi internet.

Karakteristik Cybercrime

Dalam perkembangannya kejahatan konvensional cybercrime dikenal dengan :
1. Kejahatan kerahbiru
2. Kejahatan kerah putih

Cybercrime memiliki karakteristik unik yaitu :
1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan

Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka cybercrime diklasifikasikan :

1. Cyberpiracy : Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
2. Cybertrespass : Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau indifidu.
3. Cybervandalism : Penggunaan teknologi computer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data dikomputer.
4. Perkiraan perkembangan cyber crime di masa depan dapat diperkirakan perkembangan kejahatan cyber kedepan akan semakin meningkat seiring dengan perkembangan teknologi atau globalisasi dibidang teknologi informasi dan komunikasi, sebagai berikut :

1. **Denial of Service Attack**. Serangan tujuan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna jasa internet yang sah. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan data sampah yang tidak perlu bagi orang yang dituju. Pemilik situs web menderita kerugian, karena untuk mengendalikan atau mengontrol kembali situs web tersebut dapat memakan waktu tidak sedikit yang menguras tenaga dan energi.
1. **Hate sites.** Situs ini sering digunakan oleh hackers untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para “ekstrimis” untuk menyerang pihak-pihak yang tidak disenanginya. Penyerangan terhadap lawan atau opponent ini sering mengangkat pada isu-isu rasial, perang program dan promosi kebijakan

ataupun suatu pandangan (isme) yang dianut oleh seseorang / kelompok, bangsa dan negara untuk bisa dibaca serta dipahami orang atau pihak lain sebagai "pesan" yang disampaikan.

3. **Cyber Stalking** adalah segala bentuk kiriman e-mail yang tidak dikehendaki oleh user atau junk e-mail yang sering memakai folder serta tidak jarang dengan pemaksaan. Walaupun e-mail "sampah" ini tidak dikehendaki oleh para user.

Jenis-jenis Cybercrime

1. Jenis-jenis cybercrime berdasarkan jenis aktivitasnya

1. **Unauthorized Access to Computer System and Service** : Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.
2. **Illegal Contents** : Merupakan 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. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan 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.
3. **Data Forgery** : Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. **Cyber Espionage** : Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.
5. **Cyber Sabotage and Extortion** : Kejahatan ini 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. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase

tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyber-terrorism.

6. **Offense against Intellectual Property** : Kejahatan ini 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.
7. **Infringements of Privacy** : Kejahatan ini 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.
8. **Cracking** Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak system keamaanan suatu system computer 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 negative, 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.
9. **Carding** Adalah kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

1. Jenis-jenis cybercrime berdasarkan motif

1. **Cybercrime sebagai tindak kejahatan murni** : dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu system informasi atau system computer.
2. **Cybercrime sebagai tindakan kejahatan abu-abu** : dimana kejahatan ini tidak jelas antara kejahatan criminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap system informasi atau system computer tersebut.

Selain dua jenis diatas cybercrime berdasarkan motif terbagi menjadi

1. **Cybercrime yang menyerang individu** : kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermaikan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, cyberstalking, dll
2. **Cybercrime yang menyerang hak cipta (Hak milik)** : kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.
3. **Cybercrime yang menyerang pemerintah** : kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan system pemerintahan, atau menghancurkan suatu Negara.

Contoh Kasus Cybercrime

1. **Pencurian dan penggunaan *account internet* milik orang lain.**

Pencurian account ini berbeda dengan pencurian secara fisik karena pencurian dilakukan cukup dengan menangkap "*user_id*" dan "*password*" saja. Tujuan dari pencurian itu hanya untuk mencuri informasi saja. Pihak yang kecurian tidak akan merasakan kehilangan. Namun, efeknya akan terasa jika informasi tersebut digunakan oleh pihak yang tidak bertanggung jawab. Hal tersebut akan membuat semua beban biaya penggunaan account oleh si pencuri dibebankan kepada si pemilik account yang sebenarnya. Kasus ini banyak terjadi di ISP (*Internet Service Provider*). Kasus yang pernah diangkat adalah penggunaan *account* curian yang dilakukan oleh dua Warnet di Bandung.

Kasus lainnya: Dunia perbankan dalam negeri juga digegerkan dengan ulah Steven Haryanto, yang membuat situs asli tetapi palsu layanan perbankan lewat Internet BCA. Lewat situs-situs "Aspal", jika nasabah salah mengetik situs asli dan masuk ke situs-situs tersebut, identitas pengguna (user ID) dan nomor identifikasi personal (PIN) dapat ditangkap. Tercatat 130 nasabah tercuri data-datanya, namun menurut pengakuan Steven pada situs Master Web Indonesia, tujuannya membuat situs plesetan adalah agar publik memberi perhatian pada kesalahan pengetikan alamat situs, bukan mengeruk keuntungan.

Persoalan tidak berhenti di situ. Pasalnya, banyak nasabah BCA yang merasa kehilangan uangnya untuk transaksi yang tidak dilakukan. Ditengarai, para nasabah itu kebobolan karena menggunakan fasilitas Internet banking lewat situs atau alamat lain yang membuka link ke Klik BCA, sehingga memungkinkan user ID dan PIN pengguna diketahui. Namun ada juga modus lainnya, seperti tipuan nasabah telah memenangkan undian dan harus mentransfer sejumlah dana lewat Internet dengan cara yang telah ditentukan penipu ataupun saat kartu ATM masih di dalam mesin tiba-tiba ada orang lain menekan tombol yang ternyata mendaftarkan nasabah ikut fasilitas Internet banking, sehingga user ID dan password diketahui orang tersebut.

Modus kejahatan ini adalah penyalahgunaan *user_ID* dan *password* oleh seorang yang tidak punya hak. Motif kegiatan dari kasus ini termasuk ke dalam *cybercrime* sebagai kejahatan "abu-abu". Kasus *cybercrime* ini merupakan jenis *cybercrime uncauthorized access* dan *hacking-cracking.* Sasaran dari kasus ini termasuk ke dalam jenis *cybercrime* menyerang hak milik (*against property*). Sasaran dari kasus kejahatan ini adalah *cybercrime* menyerang pribadi (*against person*).

Beberapa solusi untuk mencegah kasus di atas adalah:

- Penggunaan enkripsi untuk meningkatkan keamanan.

Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (*plaintext* diubah menjadi *chipertext*). Untuk meningkatkan keamanan authentication (pengunaan *user_id* dan *password*), penggunaan enkripsi dilakukan pada tingkat socket. Hal ini akan membuat orang tidak bias menyadap data atau transaksi yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang popular adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh Nerscape. Selain server WWW dari netscape, server WWW dari Apache juga dapat dipakai karena dapat dikonfigurasikan agar memiliki fasilitas SSL dengan menambahkan software tambahan, sperti *open* SSL.

- Penggunaan Firewall

Tujuan utama dari firewall adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar dan masuk harus melalui atau melewati firewall. Firewall bekerja dengan mengamati paker *Intenet Protocol* (IP) yang melewatinya.

- Perlunya CyberLaw

Cyberlaw merupakan istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain adalah hukum TI (Low of IT), Hukum Dunia Maya (Virtual World Law) dan hukum Mayantara.

- Melakukan pengamanan sistem melalui jaringan dengan melakukan pengaman FTP, SMTP, Telnet dan pengaman Web Server.

2. Penyerangan terhadap jaringan internet KPU

Jaringan internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat *down* (terganggu) beberapa kali. KPU menggandeng kepolisian untuk mengatasi hal tersebut. "*Cybercrime* kepolisian juga sudah membantu. Domain kerjasamanya antara KPU dengan kepolisian", kata Ketua Tim Teknologi Informasi KPU, Husni Fahmi di Kantor KPU, Jalan Imam Bonjol, Menteng , Jakarta Pusat (15 April 2009).

Menurut Husni, tim kepolisian pun sudah mendatangi Pusat Tabulasi Nasional KPU di Hotel Brobudur di Hotel Brobudur, Jakarta Pusat. Mereka akan mengusut adanya dugaan kriminal dalam kasus kejahatan dunia maya dengan cara meretas. "Kamu sudah melaporkan semuanya ke KPU. *Cybercrime* sudah datang," ujarnya. Sebelumnya, Husni menyebut sejak tiga hari dibuka, Pusat Tabulasi berkali-kali diserang oleh peretas." Sejak hari lalu dimulainya perhitungan tabulasi, samapai hari ini kalau dihitung-hitung, sudah lebuh dari 20 serangan", kata Husni, Minggu(12/4).

Seluruh penyerang itu sekarang, kata Husni, sudah diblokir alamat IP-nya oleh PT. Telkom. Tim TI KPU bias mengatasi serangan karena belajar dari pengalamn 2004 lalu. "Memang sempat ada yang ingin mengubah tampilan halaman tabulasi nasional hasil pemungutan suara milik KPU. Tetapi segera kami antisipasi."

Kasus di atas memiliki modus untuk mengacaukan proses pemilihan suara di KPK. Motif kejahatan ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja untuk melakukan pengacauan pada tampilan halaman tabulasi nasional hasil dari Pemilu. Kejahatan

kasus *cybercrime* ini dapat termasuk jenis *data forgery*, *hacking-cracking*, *sabotage and extortion*, atau *cyber terorism*. Sasaran dari kasus kejahatan ini adalah *cybercrime* menyerang pemerintah (*against government*) atau bisa juga *cybercrime* menyerang hak milik (*against property*).

Beberapa cara untuk menanggulangi dari kasus:

- Kriptografi : seni menyandikan data. Data yang dikirimkan disandikan terlebih dahulu sebelum dikirim melalui internet. Di komputer tujuan, data dikembalikan ke bentuk aslinya sehingga dapat dibaca dan dimengerti oleh penerima. Hal ini dilakukan supaya pihak-pihak penyerang tidak dapat mengerti isi data yang dikirim.
- Internet Farewell: untuk mencegah akses dari pihak luar ke sistem internal. Firewall dapat bekerja dengan 2 cara, yaotu menggunakan filter dan proxy. Firewall filter menyaring komunikasi agar terjadi seperlunya saja, hanya aplikasi tertentu saja yang bisa lewat dan hanya komputer dengan identitas tertentu saja yang bisa berhubungan. Firewall proxy berarti mengizinkan pemakai dalam untuk mengakses internet seluas-luasnya, tetapi dari luar hanya dapat mengakses satu komputer tertentu saja.
- Menutup service yang tidak digunakan.
- Adanya sistem pemantau serangan yang digunakan untuk mengetahui adanya tamu/seseorang yang tak diundang (*intruder*) atau adanya serangan (*attack*).
- Melakukan *back up* secara rutin.
- Adanya pemantau integritas sistem. Misalnya pada sistem UNIX adalah program *tripwire*. Program ini dapat digunakan untuk memantau adanya perubahan pada berkas.
- Perlu adanya *cyberlaw*: *Cybercrime* belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.
- Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.

3. Kejahatan kartu kredit yang dilakukan lewat transaksi online di Yogyakarta

Polda DI Yogyakarta menangkap lima carder dan mengamankan barang bukti bernilai puluhan juta, yang didapat dari merchant luar negeri. Begitu juga dengan yang dilakukan mahasiswa sebuah perguruan tinggi di Bandung, Buy alias Sam. Akibat perbuatannya selama setahun, beberapa pihak di Jerman dirugikan sebesar 15.000 DM (sekitar Rp 70 juta).

Para carder beberapa waktu lalu juga menyadap data kartu kredit dari dua outlet pusat perbelanjaan yang cukup terkenal. Caranya, saat kasir menggesek kartu pada waktu pembayaran, pada saat data berjalan ke bank-bank tertentu itulah data dicuri.

Akibatnya, banyak laporan pemegang kartu kredit yang mendapatkan tagihan terhadap transaksi yang tidak pernah dilakukannya.

Modus kejahatan ini adalah penyalahgunaan kartu kredit oleh orang yang tidak berhak. Motif kegiatan dari kasus ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan. Hal ini dikarenakan si penyerang dengan sengaja menggunakan kartu kredit milik orang lain. Kasus *cybercrime* ini merupakan jenis *carding.* Sasaran dari kasus ini termasuk ke dalam jenis *cybercrime* menyerang hak milik (*against property*). Sasaran dari kasus kejahatan ini adalah *cybercrime* menyerang pribadi (*against person*).

Beberapa solusi untuk mencegah kasus di atas adalah:

- Perlu adanya *cyberlaw*: *Cybercrime* belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.
- Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.
- Penggunaan enkripsi untuk meningkatkan keamanan. Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (*plaintext* diubah menjadi *chipertext*). Untuk meningkatkan keamanan authentication (pengunaan *user_id* dan *password*), penggunaan enkripsi dilakukan pada tingkat socket.

Sumber:

Oleh: Nawayatamara

https://eptik9.wordpress.com/2018/05/22/contoh-kasus-cyber-crime-dan-penyelesaiannya/

Selanjutnya, sdr liat di kolom tugas..