PERTEMUAN 4
CYBERCRIME

A. Pengertian Cybercrime

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis *internet* dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalau dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat.

Pada awalnya cybercrime didefinisikan sebagai kejahatan komputer. Menurut Mandell dalam suhariyanto (2012:10) disebutkan ada dua kegiatan computer crime :

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembuanyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Pada dasarnya cybercrime meliputi tindak pidana yang berkenaan dengan sistem informasi itu sendiri juga sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

B. Karakteristik Cybercrime

Karakteristik cybercrime yaitu :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut dilakukan dalam ruang/wilayah cyber sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan melintas batas negara.

C. Bentuk-Bentuk Cybercrime

Klasifikasi kejahatan komputer :

1. Kejahatan yang menyangkut data atau informasi komputer
2. Kejahatan yang menyangkut program atau software komputer
3. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya
4. Tindakan yang mengganggu operasi komputer
5. Tindakan merusak peralatan komputer atau yang berhubungan dengan komputer atau sarana penunjangnya.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

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 melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi *Internet*/intranet.

Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker* juga telah berhasil menembus masuk ke dalam *data base* berisi data para pengguna jasa *America Online* (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang *e-commerce* yang memiliki tingkat kerahasiaan tinggi (*Indonesian Observer*, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para *hacker*, yang mengakibatkan tidak berfugsinya situs ini beberapa waktu lamanya.

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, 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 dokumendokumen penting yang tersimpan sebagai *scripless 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 karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4. Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan *internet* untuk melakukan kegiatan matamata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

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.

6. Offense against Intellectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di *Internet*. Sebagai contoh, 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 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.

D. Contoh Cybercrime

Hacker dan Cracker

Menurut mansfield, hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi.

Sedangkan cracker adalah sisi gelap dari hacker dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

Penggolongan Hacker dan Cracker

- Recreational Hackers : kejahatan yang dilakukan oleh netter tingkat pemula untuk sekedar mencoba kekurang handalan sistem sekuritas suatu perusahaan.
- Cracker/Criminal Minded Hackers : pelaku memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan pengrusakan data. Tipe kejahatan ini dapat dilakukan dengan bantuan orang dalam.
- Political Hackers : aktifis politis (hacktivist) melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendisskreditkan lawannya.

Denial Of Service Attack

Didalam keamanan komputer, Denial of Service Attack (DoS Attack) adalah suatu usaha untuk membuat suatu sumber daya komputer yang ada tidak bisa digunakan oleh para pemakainya. Secara khas target adalah high-profile web server, serangan ini mengarahkan menjadikan host halaman web tidak ada di internet. Hal ini merupakan kejahatan komputer yang melanggar kebijakan penggunaan internet yang diindikasikan oleh internet arsitecture broad (IAB).

Denial of Service Attack mempunyai dua format umum :

1. Memaksa komputer-komputer korban untuk mereset atau korban tidak bisa lagi menggunakan perangkat komputernya seperti yang diharapkannya.

2. Menghalangi media komunikasi antara para pemakai dan korban sehingga mereka tidak bisa lagi berkomunikasi.

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

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 service.
3. Berusaha untuk mencegah individu tertentu dari mengakses suatu service.
4. Berusaha untuk mengganggu service kepada suatu orang atau sistem spesifik.

Pelanggaran Piracy

Piracy adalah kemampuan dari suatu individu atau kelompok untuk memelihara urusan pribadi dan hidup mereka ke luar dari pandangan publik, atau untuk mengendalikan alir informasi tentang diri mereka.

Pembajakan software aplikasi dan lagu dalam bentuk digital (MP3, MP4, WAV dll) merupakan trend dewasa ini, software dan lagu dapat dibajak melalui download dari internet dan dicopy ke dalam CD room yang selanjutnya diperbanyak secara ilegal dan diperjual belikan secara ilegal.

Fraud

Meruapakan 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 aktivitas yang berkaitan dengan kartu kredit. Carding muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Gambling

Perjuadian tidak hanya dilakukan secara konfensional, akan tetapi perjuadian sudah marak didunia cyber yang berskala global. Dari kegiatan ini dapat diputar kembali dinegara yang merupakan "tax heaven", seperti cyman island yang merupakan surga bagi money laundering.

Jenis-jenis online gambling antara lain :

1. Online Casinos

   Pada online casinos ini orang dapat bermain Rolet, Blackjack, Cheap dan lain-lain.

2. Online Poker

   Online Poker biasanya menawarkan Texas hold 'em, Omaha, Seven-card stud dan permainan lainnya.

3. Mobile Gambling

   Merupakan perjuadian dengan menggunakan wereless device, seperti PDAs, Wereless Tabled PCs. Beberapa casino online dan poker online menawarkan pilihan mobil. GPRS, GSM Data, UMTS, I-Mode adalah semua teknologi lapisan data atas nama perjudian gesit tergantung.

Pornography dan Paedophilia

Pornography merupakan jenis kejahatan dengan menyajikan bentuk tubuh tanpa busana, erotis, dan kegiatan seksual lainnya, dengan tujuan merusak moral. Dunia cyber selain mendatangkan kemudahan dengan mengatasi kendala ruang dan waktu, juga telah menghadirkan dunia pornografi melalui news group, chat rooms, dll. Penyebarluasan

obscene materials termasuk pornography, indecent exposure. Pelecehan seksual melalui e-mail, websites atau chat programs atau biasa disebut cyber harrassment.

Data Forgery

Kejahatan ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di Internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database. Dokumen tersebut disimpan sebagai scriptless documen dengan menggunakan media internet.

E. Istilah-istilah dalam Cybercrime

Probing : aktivitas yang dilakukan untuk melihat service-service apa saja yang tersedia di server target.

Pishing : email penipuan yang seakan-akan berasal dari sebuah toko, bank atau perusahaan kartu kredit. Email ini mengajak anda untuk melakukan berbagai hal, misalnya memverifikasi informasi kartu kredit, mengupdate password dan lainnya.

Cyber Espionage :kejahatan yang memanfaatkan internet untuk melakukan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran.

Offence Against Intelectual Property : kejahatan yang ditunjukkan terhadap HAKI yang dimiliki pihak lain di Internet.

F. Wajah Kasus Indonesia

- Money Laundering erat kaitannya dengan kegiatan mentransfer dana. Kegiatan transfer dana itu sendiri saat ini banyak dilakukan dengan menggunakan teknologi, semacam wire transfer, ATM, dan masih banyak lagi. Bahkan saat ini metode transfer dana yang banyak digunakan karena sangat cepat adalah dengan menggunakan RTGS (Real Time Gross Settlement)

- Ketika krisis di Timor-Timur sempat terjadi peperangan antara hacker indonesia dan australia. Serta ketika hubungan Indonesia dan Malaysia yang memanas karena masalah perbatasan. Beberapa situs pemerintah Malaysia sempat didevace oleh Hakcer Indonesia, dan dari Malayasia juga membalas dengan mendevace situs pemerintah daerah di Indonesia
- Dani Firmansyah, konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya menjadi nama-nama "unik", seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection(pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004