Cybercrime

Destra Bintang Perkasa 13511057

Kemajuan teknologi telah membentuk kemudahan yang luar biasa bagi kehidupan manusia di jaman sekarang ini. Internet adalah salah satu contohnya. Dengan adanya internet, kini mempelajari suatu hal yang belum bisa kita lakukan menjadi sangat mudah. Dengan Google, kita bisa mencari informasi apapun. Dengan Facebook, kita dapat mencari teman lama yang sudah tidak pernah ada kontak dengan mudah. Bahkan dengan Youtube, kita dapat melihat orang lain melakukan hal yang kita belum pernah lakukan, melihatnya mengajarkan pada kita, sambil kita mempraktikannya langsung. Namun kemudahan itu bukan semuanya yang kita dapat. Dari kemudahan itu, masih banyak orang yang memanfaatkannya untuk kegiatan yang merugikan orang lain – Ada sebuah celah baru untuk kriminalitas. Kejahatan semacam ini kemudian disebut sebagai cybercrime.

Pada essay ini akan dijelaskan hal-hal sebagai berikut:

1. Apa itu cybercrime dan apa saja yang termasuk didalamnya
2. Kaitan cybercrime dengan HAKI, Privacy dan Civil Liberty.
3. Contoh kasus cybercrime yang pernah terjadi.
4. Kaitan cybercrime dengan nama Indonesia di dunia internasional.
5. Cara untuk menangani dan mencegah kejahatan tersebut terulang kembali.
6. Cara untuk memberikan edukasi terkait masalah ini.
7. Peran masyarakat umum berkaitan dengan masalah ini.

# **Apa itu cybercrime dan apa saja yang termasuk didalamnya**

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyberterrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

1. Crimes that target computer networks or devices.
2. Crimes that use computer networks to advance other criminal activities.

Pada essay ini, yang akan dibahas dari kategori satu adalah virus dan denial-of-service attack, sedangkan untuk kategori dua adalah pencurian identitas, information warfare, dan phishing scam.

1. Virus

Sebuah virus komputer adalah sebuah program malware (kode berbahaya) yang, ketika dijalankan, mereplikasi diri dengan menyisipkan salinan dirinya (mungkin diubah) ke program lain komputer, file data, atau sektor boot dari hard drive; ketika replikasi ini berhasil, daerah yang terkena kemudian dikatakan "terinfeksi". Virus sering melakukan beberapa jenis kegiatan berbahaya pada host yang terinfeksi, seperti mencuri ruang hard disk atau waktu CPU, mengakses informasi pribadi, merusak data, menampilkan pesan-pesan politik atau pesan lucu pada layar pengguna, atau spamming kontak mereka. Namun, tidak semua virus bersifat destruktif atau mencoba untuk menyembunyikan diri mereka sendiri – yang mendefinisikan karakteristik dari virus adalah bahwa mereka adalah program komputer yang replikasinya menginstal sendiri tanpa persetujuan pengguna.

1. Denial of Service Attack

Dalam komputasi, sebuah denial-of-service (DoS) atau distributed denial-of-service (DDoS) attack merupakan upaya untuk membuat mesin atau sumber daya jaringan tersedia bagi pengguna yang dimaksudkan. Meskipun sarana untuk melaksanakan, motif, dan sasaran serangan DoS dapat bervariasi, umumnya terdiri dari upaya untuk sementara atau selamanya mengganggu atau menangguhkan layanan dari sebuah host yang terhubung ke Internet. Sebagai klarifikasi, DDoS (Distributed Denial of Service) attack dikirim oleh dua orang atau lebih, atau bot sedangkan DoS (Denial of Service) attack dikirim oleh satu orang atau sistem.

1. Pencuri Identitas

Saat ini, keamanan biometrik (misalnya, scanner sidik jari, retina scan, cetak suara, dll) terbatas pada beberapa perangkat saja, tapi setelah menjadi cara utama untuk mengotentikasi account online Anda, data biometrik akan menjadi komoditas penting bagi criminal bawah tanah. Pencurian data genetik juga berarti meningkatnya risiko ketika konsumen mendaftar untuk pengujian genetik dan data mereka disimpan pada jaringan yang rentan.

1. Pembajakan Software

Pembajakan Software adalah penggunaan karya-karya (dalam hal ini software) yang dilindungi oleh hukum hak cipta tanpa izin, melanggar hak eksklusif tertentu yang diberikan kepada pemegang hak cipta, seperti hak untuk mereproduksi, mendistribusikan, menampilkan, atau melakukan pekerjaan yang dilindungi, atau membuat karya turunan. Pemegang hak cipta biasanya pencipta pekerjaan, atau penerbit atau bisnis lainnya kepada siapa hak cipta telah ditetapkan.

1. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet. Kejahatan carding banyak jenisnya yaitu antara lain: misuse (compromise) of card data, Counterfeiting, Wire Tapping dan Phishing. *Misuse (compromise) of card data* berupa penyalahgunaan kartu kredit di mana kartu tidak di presentasikan. Dalam c*ounterfeiting*, kartu palsu sudah diubah sedemikian rupa sehingga menyerupai kartu asli. Selain itu ada juga *Wire Tapping* yaitu penyadapan transaksi kartu kredit melalui jaringan komunikasi. Yang terakhir adalah *Phishing* yaitu dengan penyadapan melalui situs website aspal (asli-tapi palsu) agar personal data nasabah dapat di curi.

# **Kaitan dengan HAKI, Privacy, dan Civil Liberty**

Dari beberapa lingkup Cybercrime yang dibahas di bagian sebelumnya, terdapat beberapa hal dari cybercrime yang dapat dikaitkan degan pelanggaran HAKI, Privacy, dan Civil Liberty. Kasus yang menyangkut HAKI pada umumnya adalah tentang pembajakan software. Untuk kasus ini, Undang-undang tindak pidana telah mengaturnya dalam Pasal 72 ayat (3) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta yaitu “Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus jutarupiah)“.

Selain itu isu lain yang dapat dikaitkan dengan cyberbrime adalah *privacy* dan *civil liberty*. Hacker yang masuk ke sistem jaringan orang lain tanpa seizin pemiliknya tentu telah melanggar beberapa nilai penting yang ada pada konsep *privacy* dan *civil liberty*. Di Indonesia, pelanggaran ini diatur dalam Pasal 22 Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi, yaitu setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

a. Akses ke jaringan telekomunikasi

b. Akses ke jasa telekomunikasi

c. Akses ke jaringan telekomunikasi khusus

akan dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).”

# **Contoh Kasus Cybercrime yang Pernah Terjadi**

Salah satu kasus cybercrime yang pernah terjadi dan marak di Indonesia adalah carding. Pada tahun 2005, kejahatan ini sempat menjadi kejahatan paling popular di Indonesia. Kejahatan ini dimulai pada tahun 2001 saat internet banking diributkan oleh kasus pembobolan internet banking milik bank BCA. Pada saat itu salah satu karyawan media online (satunet.com) yang bernama Steven Haryanto (beberapa sumber menyebutkan Steven Haryono) membeli domain-domain internet dengan harga sekitar US$20 yang menggunakan nama dengan kemungkinan orang-orang salah mengetikkan dan tampilan yang sama persis dengan situs internet banking BCA, yaitu http://www.klikbca.com. Dengan demikian, jika seorang nasabah salah memasukkan alamat website menjadi, misalnya clikbca.com, maka nasabah tersebut akan masuk ke situs Steven dan Steven dapat meminta nasabah memasukkan nomor PIN atau Password nya.

Kasus ini dapat terjadi karena adanya kelalaian nasabah dalam mengetikkan alamat website, bank bersangkutan yang tidak menanggulangi hal-hal seperti ini, yang menyebabkan adanya kesempatan untuk pelaku kejahatan melakukan aksinya. Biasanya, pelaku menggunakan alamat e-mail palsu dan grafik untuk menyesatkan nasabah sehingga nasabah terpancing menerima keabsahan e-mail atau web sites. Agar tampak meyakinkan, pelaku juga seringkali memanfaatkan logo atau merk dagang milik lembaga resmi, seperti; bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi, seperti; password, PIN dan nomor kartu kredit.

Kasus carding ini sudah diatur dalam Kitab Undang Undang Hukum Pidana (KUHP) diantaranya pada Pasal 362 KUHP. Selain itu, carding juga dapat dikenakan Pasal 378 yaitu tentang penipuan.

Akibat kasus ini, Steven mendapatkan 130 data nasabah bank BCA dan dikenakan hukuman 10 tahun penjara atas perbuatannya tersebut.

# **Kaitan cybercrime dengan nama Indonesia di dunia internasional**

Berdasarkan hasil riset dari Clear Commerce Inc, sebuah perusahaan teknologi informasi (TI) yang berbasis di Texas, AS, pada tahun 2005, akibat kasus *carding* yang dijelaskan pada bagian sebelumnya Indonesia berada pada posisi ke-2 teratas sebagai negara asal carder terbanyak di dunia,setelah Ukraina. Hal ini menimbulkan preseden buruk bagi para produsen maupun distributor barang-barang yang diperjual belikan melalui internet. Sehingga banyak diantara mereka yang tidak mau mengirimkan barang pesanan di internet dengan alamat tujuan Indonesia.

# **Cara untuk Menangani dan Mencegah Kejahatan Tersebut Terulang Kembali**

Salah satu cara yang dapat digunakan agar memperkecil peluang cybercrime adalah dengan menggunakan Secure Socket Layer saat ingin membuat koneksi di internet. Hal ini dapat dengan mudah dilakukan dengan mengakses https alih-alih http untuk situs yang anda mau kunjungi. Selain itu, jangan lupa buat juga sertifikat SSL untuk aplikasi web yang sedang dikembangkan. Terakhi, itu, gunakan juga One Time Password agar anda tidak perlu mengingat dan memasukkan password secara manual yang sangat memungkinkan adanya “kebocoran” pada data yang Anda masukkan. Pastikan juga anda telah logout setiap kali anda telah selesai menggunakan akun anda di dinternet.

# **Cara untuk Memberikan Edukasi Terkait Masalah Ini**

Beberapa tahun kedepan, cybercrime mungkin sudah bukan masalah yang hanya berkaitan dengan komputer lagi. Dengan adanya mobil pintar yang semuanya terkomputerisasi, alat kesehatan yang sekarang bertenaga komputer, pengenal identitas seperti scanner retina, sidik jari, akan menjadi sasaran dari cybercrime. Untuk ini masyarakat harus diberikan edukasi terkait isu cybercrime ini. Edukasi dapat berupa seminar keamanan informasi pribadi dan data. Untuk masyrakat umum sangat penting adanya pendidikan agar tidak menyebarkan password ke orang lain, mengganti password secara berkala, dan tidak dengan mudah menyebarkan data pribadi pada form-form atau kuesioner tertentu. Untuk pengembang aplikasi, sangat penting adanya seminar tentang pentingnya menjaga data-data pengguna aplikasi yang mereka buat.

# **Peran Masyarakat Umum**

Masyarakat umm juga bisa berperan dalam memerangi cybercrime dimulai dari diri sendiri.Tidak seharusnya kita membeli software bajakan. Dengan kita menggunakan software bajakan, kita telah merugikan orang yang membuat software. Menjualnya untuk kepentingan komersil tentunya lebih tidak seharusnberperan dalam memerangi cybercrime dimulai dari diri sendiri.Tidak seharusnya kita membeli software bajakan. Dengan kita menggunakan software bajakan, kita telah merugikan orang yang membuat software. Menjualnya untuk kepentingan komersil tentunya lebih tidak seharusnya lagi. Kita masih bisa menggunakan software yang gratis atau open source.

# **Referensi**

http://101102109-ebusiness.blogspot.com/2012/11/informasi-klik-bca-phishing.html

http://echanharvandha22.blogspot.com/2014/03/contoh-kasus-cyber-crime\_1391.html

http://infokejahatanit.blogspot.com/2013/04/cyber-crime.html

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York.

"Types of DDoS Attacks". Distributed Denial of Service Attacks (DDoS) Resources, Pervasive Technology Labs at Indiana University. Advanced Networking Management Lab (ANML). December 3, 2009.

Bell, David J. et al, ed. (2004). "Virus". Cyberculture: The Key Concepts. Routledge. p. 154.

http://cybercrimeetikainformasi.blogspot.com/2013/04/undang-undang-cybercrime-di-indonesia.html

criminalita-informatica.blogspot.com/2013/05/undang-undang-yang-mengatur-tentang.html

Ram D. Gopal and G. Lawrence Sanders. “International Software Piracy: Analysis of Key Issues and Impacts.” Information Systems Research 9, no. 4 (December 1998): 380–397.

http://faniyaulia.blogspot.com/2014/03/kasus-kasus-cybercrime-atau-computer.html