UNIVERSITAS MERCU BUANA

MODUL PERKULIAHAN

EDP Audit

Kejahatan Komputer

(*Cuber Crime*)

Fakultas	Program Studi	Tatap Muka	Kode MK	Disusun Oleh
Ekonomi dan Bisnis	S1 Akuntansi	13	32049	Hidayatullah,SE.,MSi.,AK.,CA

Abstract

Modul ini membahas tentang Kejahatn computer dan beberapa kasus yang terjadi sehubungan dengan kejahatn computer serta cara menanganinya supaya terhindar dari kejahat computer.

Kompetensi

Mahasiswa mampu pememahami tantang hal-hal yang terkait dengan kejahatan computer dan bagaimana cara menanggulanginya..

Pengantar

Selama dua puluh tahun terakhir, pengguna komputer tidak bermoral terus menggunakan komputer untuk melakukan kejahatan; ini memiliki orang sangat terpesona dan membangkitkan perasaan campuran kekaguman dan ketakutan. Fenomena ini telah melihat peningkatan yang canggih dan belum pernah terjadi sebelumnya baru-baru dan telah menyerukan respon cepat dalam memberikan hukum yang akan melindungi ruang cyber dan penggunanya. Tingkat kecanggihan sudah tinggi ke titik menggunakan sistem untuk melakukan pembunuhan dan kekacauan lainnya. Pembunuhan pertama yang tercatat maya yang dilakukan di Amerika Serikat tujuh tahun yang lalu menurut Indian Express, Januari 2002 "harus dilakukan dengan bawah don di rumah sakit untuk menjalani operasi kecil. Goon saingannya menyewa seorang ahli komputer yang diubah resep nya melalui hacking sistem komputer rumah sakit. Dia diberikan resep diubah oleh perawat yang tidak bersalah, ini mengakibatkan kematian pasien "

Karya ini bertujuan untuk menentukan konsep cyber crime, mengidentifikasi alasan untuk kejahatan cyber, bagaimana hal itu dapat diberantas, melihat orang-orang yang terlibat dan alasan untuk keterlibatan mereka, kita akan melihat bagaimana cara terbaik untuk mendeteksi mail kriminal dan dalam kesimpulan , mengajukan rekomendasi yang akan membantu dalam memeriksa tingkat peningkatan cyber kejahatan dan penjahat.

Definisi dan Gambaran

WHAT IS CYBER – CRIME?

Cyber-kejahatan menurut definisi adalah tindakan berbahaya yang dilakukan dari atau terhadap komputer atau jaringan, hal itu berbeda menurut McConnell Internasional, "dari sebagian besar kejahatan terestrial dalam empat cara: mereka mudah untuk belajar bagaimana melakukan, mereka membutuhkan sedikit sumber daya relatif terhadap potensi kerusakan yang disebabkan, mereka dapat dilakukan di wilayah hukum tanpa secara fisik hadir di dalamnya dan keempat, mereka sering tidak jelas ilegal. "

Definisi lain diberikan oleh Direktur Kejahatan Komputer Pusat Penelitian (CCRC) selama wawancara pada 27 April 2004, adalah bahwa "kejahatan cyber ('komputer kejahatan') adalah setiap perilaku ilegal diarahkan dengan cara operasi elektronik yang menargetkan keamanan sistem komputer dan data diproses oleh mereka. "Pada intinya, kejahatan cyber adalah kejahatan yang dilakukan di ruang virtual dan ruang virtual kuno dengan cara bahwa informasi tentang orang, benda, fakta, peristiwa, fenomena atau proses direpresentasikan dalam matematika, simbol atau cara lain dan ditransfer melalui jaringan lokal dan global

Dari atas, kita dapat menyimpulkan bahwa kejahatan cyber hubungannya dengan perusakan malapetaka pada data komputer atau jaringan melalui intersepsi, gangguan atau kerusakan data atau sistem tersebut. Ini melibatkan melakukan kejahatan terhadap sistem komputer atau penggunaan komputer dalam melakukan kejahatan.

CAUSES OF CYBER – CRIME

Ada banyak alasan mengapa penjahat cyber melakukan kejahatan cyber, kepala di antara mereka adalah tiga tercantum di bawah ini:

- kejahatan Cyber dapat dilakukan demi pengakuan. Hal ini pada dasarnya dilakukan oleh anak muda yang ingin diperhatikan dan merasa di antara sekelompok orang-orang besar dan tangguh dalam masyarakat. Mereka tidak bermaksud menyakiti orang tertentu; mereka jatuh ke dalam kategori Idealis; yang hanya ingin berada dalam sorotan.

- Penyebab lain dari kejahatan cyber adalah untuk membuat uang cepat. Kelompok ini adalah keserakahan termotivasi dan penjahat karir, yang mengutak-atik data pada bersih atau sistem terutama, e-commerce, informasi data e-banking dengan tujuan tunggal melakukan penipuan dan menipu uang dari pelanggan yang tidak curiga.

- Ketiga, kejahatan cyber dapat dilakukan untuk melawan penyebab orang berpikir ia percaya di; menyebabkan ancaman dan paling sering kerusakan yang mempengaruhi penerima negatif. Ini adalah yang paling berbahaya dari semua penyebab kejahatan cyber. Mereka melibatkan percaya bahwa mereka berjuang hanya menyebabkan dan tidak keberatan siapa atau apa yang mereka menghancurkan dalam pencarian mereka untuk mendapatkan tujuan mereka tercapai. Ini adalah cyber teroris.

HOW TO ERADICATE CYBER – CRIME

Penelitian telah menunjukkan bahwa tidak ada hukum dapat diletakkan di tempat untuk secara efektif membasmi momok kejahatan cyber. Upaya telah dilakukan secara lokal dan internasional, tetapi hukum-hukum ini masih memiliki ditembak-kedatangan. Apa yang merupakan kejahatan di negara mungkin tidak di tempat lain, jadi ini selalu membuat mudah bagi penjahat cyber untuk pergi bebas setelah ditangkap.

Tantangan-tantangan ini meskipun, pemerintah harus dalam kasus idealis, melawan mereka melalui pendidikan bukan hukum. Telah terbukti bahwa mereka membantu perusahaan-perusahaan besar dan pemerintah melihat lubang keamanan yang penjahat karir atau bahkan cyber teroris bisa digunakan untuk menyerang mereka di masa depan. Paling sering, perusahaan melibatkan mereka sebagai konsultan untuk membantu mereka membangun keamanan yang kuat untuk sistem dan data mereka. "The Idealis sering membantu masyarakat: melalui tindakan yang sangat mediatised dan individual tidak berbahaya, mereka membantu organisasi penting untuk menemukan lubang keamanan berteknologi tinggi mereka ...." Penegakan hukum pada mereka hanya dapat memicu masalah, karena mereka tidak akan berhenti tapi akan ingin menentang hukum. "Selain itu, jika tujuan dari undang-undang cyber crime adalah untuk memberantas kejahatan cyber, itu

mint juga membasmi bukan budaya baru ...." Investasi di bidang pendidikan adalah cara yang lebih baik untuk mencegah tindakan mereka.

Cara lain memberantas kejahatan cyber adalah untuk menyelaraskan kerjasama internasional dan hukum, ini berlaku untuk keserakahan termotivasi dan cyber-teroris. Mereka tidak bisa diperangi oleh pendidikan, karena mereka sudah mapan penjahat, sehingga mereka tidak dapat berperilaku. Satu-satunya cara yang tepat untuk melawan mereka adalah dengan memberlakukan undang-undang baru, harmonisasi peraturan perundang-undangan internasional dan mendorong koordinasi dan kerjasama antara lembaga penegak hukum nasional.

WHO ARE INVOLVED

Mereka yang terlibat dalam melakukan kejahatan cyber dalam tiga kategori dan mereka adalah:

- THE IDEALISTS (Teenager). Mereka biasanya tidak terlatih atau terampil, tetapi anak-anak antara usia 13-26 yang mencari pengakuan sosial. Mereka ingin menjadi sorotan media. Tindakan mereka secara global damageable tapi secara individu diabaikan. "Seperti menyangkal banyak penting e-commerce server pada bulan Februari 2000 dikatakan telah menyebabkan kerusakan yang tinggi untuk perusahaan-perusahaan ini." Paling sering mereka menyerang sistem dengan virus yang mereka ciptakan; bahaya yang sebenarnya mereka untuk setiap individu relatif diabaikan. Pada usia 26-26 ketika mereka telah matang dan memahami berat dari tindakan mereka, mereka kehilangan minat dan berhenti.

- THE KESERAKAHAN - TERMOTIVASI (Penjahat Karir). Jenis penjahat cyber berbahaya karena mereka biasanya tidak bermoral dan siap untuk melakukan semua jenis kejahatan, asalkan membawa uang untuk mereka. "Mereka mulai pornografi anak sering disebut cyber pornografi yang englobes pornografi legal dan ilegal di internet." Mereka biasanya sangat cerdas dan terorganisir dan mereka tahu bagaimana untuk melarikan diri dari lembaga penegak hukum. Ini penjahat cyber yang melakukan kejahatan pedih dan kerusakan dan unscrupulousness mereka, terutama pada anak-pornografi dan cyber perjudian adalah ancaman serius bagi masyarakat. Contoh untuk menunjukkan betapa seriusnya ancaman mereka berpose

untuk masyarakat adalah "korban dari bank Eropa Antigua dikatakan telah kehilangan lebih dari $ 10 juta" "... pencurian rahasia dagang berharga: kode sumber dari jendela mikro-lunak populer sistem eksplorasi oleh hacker berbasis Rusia bisa menjadi sangat berbahaya ... hacker bisa menggunakan kode untuk memecahkan semua firewall dan menembus jarak jauh setiap komputer dilengkapi dengan jendela dikonfirmasi. Penggunaan lain bisa menjadi penjualan kode untuk pesaing. "

- CYBER THE - Teroris. Mereka adalah kelompok terbaru dan paling berbahaya. Motif utama mereka bukan hanya uang tetapi juga penyebab spesifik mereka membela. Mereka biasanya terlibat dalam mengirim mail ancaman, menghancurkan data yang disimpan dalam sistem informasi terutama pemerintah hanya untuk mencetak poin mereka. Ancaman cyber-terorisme dapat dibandingkan dengan orang-orang dari ancaman senjata nuklir, bakteriologi atau kimia. Masalah menyedihkan ini adalah bahwa mereka tidak memiliki batas negara; dapat beroperasi dari setiap tempat di dunia, dan ini membuat sulit bagi mereka untuk terjebak. Yang paling ingin cyber teroris Osama Bin Laden yang dikatakan "menggunakan stegranography untuk menyembunyikan pesan rahasia dalam gambar, misalnya, gambar Aishwarya Rai host di website bisa berisi pesan tersembunyi untuk meledakkan sebuah bangunan." Sebuah fakta mengejutkan adalah bahwa pesan-pesan tersembunyi tidak mengubah bentuk, ukuran atau tampilan gambar asli dengan cara apapun.

HOW TO DETECT A CRIMINAL MAIL

Sebuah email kriminal biasanya dikirim ke jaringan dengan tujuan baik merusak sistem atau melakukan penipuan. Cara untuk mendeteksi mail tersebut adalah dengan meletakkan langkah-langkah keamanan di tempat yang akan mendeteksi pola kriminal dalam jaringan. Berita Cerita oleh Paul Roberts, dari IDG News Service mengatakan bahwa Unisys Suite memiliki sistem yang disebut "Unisys Sistem Pemantau Risiko Aktif (ARMS) yang membantu bank dan organisasi lain pola tempat kejadian tampaknya tidak berhubungan yang menambahkan hingga kegiatan kriminal." Actimize Teknologi Ltd yang berbasis di New York telah mengembangkan teknologi yang memungkinkan organisasi untuk melakukan kompleks data mining dan analisis informasi dan transaksi data yang disimpan tanpa perlu menyalinnya ke sebuah gudang data yang terpisah. "Perangkat lunak actimize berjalan pada

platform Microsoft Corp Windows NT atau Windows 2002 dan dapat dikembangkan pada server hardware standar dengan baik 4-8 prosesor, kata Katz."

Eric J. Sinrod dalam artikelnya "Apa Up Dengan Pemerintah Mining Data 'menyatakan bahwa Amerika Serikat" Pemerintah Federal telah menggunakan teknik data mining untuk berbagai tujuan, dari mencoba untuk meningkatkan pelayanan kepada mencoba untuk mendeteksi pola dan kegiatan teroris. "Yang paling cara yang efektif untuk mendeteksi mail pidana adalah untuk memberikan gadget keamanan, mendidik karyawan tentang cara menggunakannya, dan berada di siaga untuk kiriman tersebut, di atas semua, pastikan tidak ada lubang keamanan yang tersisa tanpa pengawasan untuk.

CONCLUSION

Telah disimpulkan dari penelitian ini bahwa ketergantungan pada hukum terestrial masih pendekatan belum teruji meskipun kemajuan yang dibuat di banyak negara, mereka masih mengandalkan hukum terestrial standar untuk mengadili kejahatan cyber dan hukum-hukum ini adalah ketetapan kuno yang telah ada sebelum kedatangan dari dunia maya. Juga hukuman yang lemah membatasi pencegahan: negara dengan undang-undang pidana diperbarui masih memiliki hukuman yang lemah pada undang-undang pidana; ini tidak dapat mencegah penjahat melakukan kejahatan yang memiliki dampak ekonomi dan sosial skala besar di masyarakat. Juga tambal sulam global hukum menciptakan sedikit kepastian; sedikit konsensus ada di antara negara-negara mengenai kejahatan yang perlu disahkan terhadap. Perlindungan diri tetap baris pertama pertahanan dan model pendekatan yang dibutuhkan oleh sebagian besar negara; terutama di negara berkembang mencari model untuk diikuti. Mereka menyadari pentingnya melarang tindakan yang berkaitan dengan komputer berbahaya pada waktu yang tepat atau dalam rangka untuk mempromosikan lingkungan yang aman untuk e-commerce.

Kejahatan cyber dengan kompleksitas yang telah terbukti sulit untuk memerangi karena sifatnya. Memperluas aturan hukum dalam dunia maya adalah langkah penting untuk menciptakan lingkungan yang dapat dipercaya untuk orang dan bisnis. Karena ketentuan hukum tersebut untuk secara efektif mencegah kejahatan cyber masih bekerja di sebuah kemajuan, menjadi perlu untuk individu dan badan hukum untuk fashion cara-cara

menyediakan keamanan untuk sistem dan data mereka. Untuk memberikan ini perlindungan diri, organisasi harus fokus pada pelaksanaan rencana keamanan cyber menangani orang, masalah proses dan teknologi, lebih banyak sumber daya harus dimasukkan ke dalam untuk mendidik karyawan organisasi pada praktek keamanan, "mengembangkan rencana menyeluruh untuk menangani data sensitif, catatan dan transaksi dan memasukkan keamanan yang kuat teknologi--seperti firewall, software anti-virus, alat deteksi intrusi dan otentikasi services--. "

Dengan rekomendasi cara, jenis-jenis tindakan yang disarankan berikut sifat lemah perlindungan hukum global melawan kejahatan cyber:

- Perusahaan harus mengamankan informasi jaringan mereka. Ketika organisasi memberikan keamanan untuk jaringan mereka, menjadi mungkin untuk menegakkan hukum hak milik dan hukuman bagi siapa pun yang mengganggu properti mereka.
- Hukum harus berlaku untuk pemerintah cyber-crime Nasional masih menjadi kewenangan utama yang dapat mengatur perilaku kriminal di sebagian besar tempat di dunia. Jadi upaya sadar oleh pemerintah untuk menempatkan hukum di tempat untuk mengatasi kejahatan cyber akan cukup diperlukan.
- Harus ada hubungan simbiosis antara perusahaan, pemerintah dan masyarakat sipil untuk memperkuat kerangka hukum untuk keamanan cyber. Tindakan harus kejahatan di setiap wilayah hukum sebelum dapat dituntut di perbatasan. Bangsa harus menentukan cyber kejahatan dengan cara yang sama, untuk memungkinkan mereka lewat undang-undang yang akan melawan kejahatan cyber secara lokal dan internasional.

Daftar Pustaka

1. **Cyber Crime is here to stay**. Indian Express, January 2002 http://www.asianlaws.org/press/cybercrime.htm
2. **Cyber-Crime… and Punishment? Archaic Laws threaten Global Information.** December, 2000 www.mcconnellinternational.com/services.cybercrime.htm,
3. [1] Golubev's interview. http://www.crime-research.org/Golubev_interview_052004/

4. [1] Prof. Hammond, Allen. **The 2001 Council of European Convention on Cyber-Crime: an Efficient Tool to Fight Crimes in Cyber-Space?** June, 2001, http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond. COEConvention.Cyber-crime.pdf

[1] Ibid

[1] Ibid

[1] Ibid

[1] Ibid

[1] Ibid

[1] **Cyber Crime is here to stay**. Indian Express January 2002 http://www.asianlaws.org/press/cybercrime.htm

[1] Katz, Eli **Unisys Suite Aims To Detect Criminal patterns,** June 10, 2003 http://www.computerworld.com/industrytopics/financial/story/0,10801,81979,00.html

[1] Ibid

[1] Sinrod, J. Eric. **What's Up With Government Data Mining?** September 6, 2004, http://www.ustoday.com/tech/columnist/ericjsinrod/2004-06-09-sinrod_x.htm

[1] **Cyber-Crime… and Punishment? Archaic Laws threaten Global Information.** December, 2000 www.mcconnellinternational.com/services.cybercrime.htm,

1.