ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.2 No.1 Tahun 2023
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2023

Jenis dan Dampak Cyber Crime

Types and Effects of Cyber Crime

Cahyo Hidayatullah
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
vonixgame22@gmail.com

Abstract

A cyberattack or cyber attack is a type of offensive maneuver used by a, individual, group or organization that targets computer information systems, infrastructure, computer networks and personal computer devices through malicious actions that usually originate from anonymous sources that steal, modify or destroy. specific targets by breaking into vulnerable systems. This can be labeled as a cyber campaign, cyber war or cyber terrorism in different contexts. Cyber attacks can range from installing spyware on PCs to trying to destroy an entire country's infrastructure. Cyber attacks have become as sophisticated and dangerous as the recently demonstrated Stuxnet worm.20 User behavior analysis and Security Information and Event Management (SIEM) are used to prevent these attacks. Cyber extortion occurs when a website, email server or computer systems are subject to or threatened with repeated denial of service (DoS) or other attacks by malicious hackers.

Keywords*: Cyber Crime, Impacts of Cyber Crime, Hacking*

Abstrak

Serangan dunia maya atau *Cyber Crime* adalah jenis manuver ofensif yang digunakan oleh suatu, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer, dan perangkat komputer pribadi melalui tindakan jahat yang biasanya berasal dari sumber anonim yang mencuri, memodifikasi atau menghancurkan. target spesifik dengan membobol sistem yang rentan. Hal ini dapat disebut sebagai kampanye dunia maya, perang dunia maya, atau terorisme dunia maya dalam konteks yang berbeda. Serangan dunia maya dapat berkisar dari memasang spyware di PC hingga mencoba menghancurkan infrastruktur seluruh negara. Serangan dunia maya telah menjadi secanggih dan berbahaya seperti worm Stuxnet yang baru-baru ini didemonstrasikan.20 Analisis perilaku pengguna dan Manajemen Informasi dan Peristiwa Keamanan (SIEM) digunakan untuk mencegah serangan ini.Pemerasan dunia maya terjadi ketika situs web, server email, atau sistem komputer tunduk atau terancam dengan penolakan berulang layanan (DoS) atau serangan lain oleh hacker jahat.

Kata kunci: Kejahatan Dunia Maya, Dampak Kejahatan Dunia Maya, Peretasan

Pendahuluan

Cyber crime adalah kejahatan yang menggunakan teknologi informasi dan merupakan salah satu bentuk kejahatan transnasional tidak mengenal batas negara, tanpa kekerasan (non violence), tidak ada kontak fisik (no physical contact) dan tanpa nama Karakteristik Cyber crime yang membuat para pelaku Cyber Crime sangat sulit dilacak dan unsur pidananya sulit dibuktikan, apalagi keterbatasan regulasi.[1]

Cybercrime atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (net-work).1 Komputer mungkin telah digunakan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.2 Cybercrimes 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 (Bluetooth / SMS / MMS)"[2].

Istilah kejahatan dunia maya dapat didefinisikan sebagai tindakan yang dilakukan atau dihilangkan dengan melanggar hukum yang melarang atau memerintahkannya dan yang hukumannya dijatuhkan atas keyakinan. Dengan kata lain, kejahatan dunia maya sebagai "Aktivitas kriminal yang terkait langsung dengan penggunaan komputer, khususnya pelanggaran ilegal ke dalam sistem komputer atau database orang lain, manipulasi atau pencurian data yang disimpan atau online, atau sabotase peralatan dan data." Ruang internet atau ruang siber tumbuh sangat cepat dan sebagai kejahatan dunia maya.[3]

Internet dan teknologi informasi merupakan inovasi baru pada dekade terakhir ini dan sangat mempengaruhi kehidupan manusia. Beberapa aktifitas manusia berubah secara signifikan dengan mengambil keuntungan dari efisiensi, efektifitas, dan mobilitas. Sayangnya, kemajuan teknologi ini juga memperkenalkan permasalahanpermasalahan baru saat digunakan secara tidak tepat atau menyalahi dari yang semestinya. Kejahatan cyber (cybercrime) adalah bentuk ancaman baru yang belum pernah ada sebelumnya pada masyarakat dunia. Saat ini, meskipun hukum pidana konvensional sebagaimana yang berlaku di Indonesia dapat digunakan hakim sebagai dasar hukum untuk mengadili pelaku cybercrime, tapi dalam praktik banyak sekali keterbatasannya, baik dari sisi unsur tindak pidana maupun pertanggung jawaban pidananya. Akibatnya, banyak pelaku yang lolos dari jeratan hukum, atau kalaupun dijatuhi pidana berdasarkan hasil penelitian semua pelaku dijatuhi pidana penjara. Dalam tataran filosofis, teori teoritis, normatif, maupun empiris, pidana penjara merupakan suatu jenis pidana yang mempunyai banyak kelemahan, karena pelaksanaan pidana penjara, khususnya di Indonesia kurang memadai.[4]

Metode Penelitian

Metode yang digunakan dalam penulisan artikel ini adalah literature riview. Yaitu sebuah pencarian literatur baik dari artikel nasional dan internasional yang dilakukan dengan database ScienceDirect dan Google Schoolar. Pencarian artikel jurnal diperoleh dari 10 artikel menggunakan kata kunci "CyberCrime" "Dampak dan jenis CyberCrime" yang diidentifikasi.

Hasil dan Pembahasan

Peretasan

Peretasan adalah salah satu bentuk pelanggaran. Ini adalah penggunaan yang tidak sah, atau akses ke, komputer atau sumber daya jaringan, yang mengeksploitasi kerentanan keamanan yang teridentifikasi dalam jaringan. Peretasan dapat digunakan untuk mengumpulkan data atau informasi pribadi yang digunakan untuk penjahat merusak situs web atau digunakan sebagai bagian dari penolakan layanan (DoS) atau serangan DDoS (lihat di bawah).
Denial of service atau serangan denial of service terdistribusi DoS dan DDoS terkait dengan membanjiri server internet dengan begitu banyak permintaan (misalnya, tautan yang telah diklik) sehingga tidak dapat merespons dengan cukup cepat. Ini dapat membebani server yang menyebabkannya macet atau macet.[3]

Spam

Spam adalah email yang tidak diminta atau 'sampah', biasanya dikirim secara massal ke penerima yang tak terhitung jumlahnya di seluruh dunia dan sering dikaitkan dengan produk farmasi atau pornografi. Email spam juga digunakan untuk mengirim email phishing atau malware dan dapat membantu memaksimalkan potensi keuntungan bagi penjahat.[3]

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 Anda, penyebaran informasi yang salah dapat digunakan.[2]

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 di tentukan dengan cara membobol sistem yang rentan.19 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 telah menjadi semakin canggih dan berbahaya seperti worm Stuxnet yang baru-baru ini didemonstrasikan.20 Analisis perilaku pengguna dan Keamanan Informasi dan Event Manajemen (Security Information and Eevent Management / SIEM) digunakan untuk mencegah serangan ini. Pakar hukum berusaha membatasi penggunaan istilah tersebut pada insiden yang menyebabkan kerusakan fisik, membedakannya dari pelanggaran data yang lebih rutin dan aktivitas hacking yang lebih luas[2].

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". Menurut Biro Investigasi Federal, 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. Lebih dari 20 kasus dilaporkan setiap bulan ke FBI dan banyak yang tidak dilaporkan untuk menjaga agar nama korban tidak keluar dan tersebar ke publik. Pelaku biasanya menggunakan serangan denial-of-service terdistribusi (distributed denial-of-service / DDoS).[2]

Cyberwarfare

Departemen Pertahanan Amerika Serikat (Department ofDefense / DoD) mencatat bahwa dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi geostrategis. Di antaranya termasuk serangan terhadap infrastruktur Estonia di tahun 2007, yang diduga oleh hacker Rusia. "Pada bulan Agustus 2008, Rusia kembali melakukan serangan cyber, kali ini dalam kampanye kinetik dan non kinetik yang terkoordinasi dan disinkron kan melawan negara Georgia. Khawatir bahwa serangan semacam itu dapat menjadi norma perang antar negara di masa depan, dampak dari konsep operasi dunia maya akan disesuaikan oleh para komandan militer di masa depan.[2]

Pencurian Data

Istilah yang digunakan untuk mendeskripsikan saat informasi disalin atau diambil secara ilegal dari bisnis atau individu lain. Umumnya, informasi ini adalah informasi pengguna seperti kata sandi, nomor jaminan sosial, informasi kartu kredit, informasi pribadi lainnya, atau informasi rahasia perusahaan lainnya. Karena informasi ini diperoleh secara tidak sah, ketika individu yang mencuri informasi ini ditangkap, kemungkinan besar dia akan dituntut secara hukum seberat-beratnya.[5]

Modifikasi Data

Privasi komunikasi sangat penting untuk memastikan bahwa data tidak dapat diubah atau dilihat saat transit. Lingkungan terdistribusi membawa serta kemungkinan bahwa pihak ketiga yang jahat dapat melakukan kejahatan komputer dengan merusak data saat berpindah antar situs.[5]

Sabotase Jaringan

'Sabotase Jaringan' atau manajer yang tidak kompeten mencoba melakukan pekerjaan orang yang biasanya mereka tangani? Bisa di atas saja, atau kombinasi dari hal-hal. Tetapi jika Verizon menggunakan bantuan anak-anak, menghalangi jalur responden pertama, maka mereka mungkin menggunakan masalah jaringan sebagai alasan untuk membuat pemerintah federal campur tangan demi kepentingan keselamatan publik. Tentu saja jika pemerintah federal memaksa orang-orang ini kembali bekerja, apa tujuan dari serikat pekerja dan pemogokan.[3]

Aktivitas kejahatan cyber yang menargetkan computer dapat menginfeksi perangkat dengan malware sehingga bisa menginfeksi perangkat. Malware juga dapat digunakan untuk menghapus, mencuri data, atau bahkan menghentikan pengguna untuk menggunakan website. Berikut ini adalah penjelasan dampak dari Cyber Crime.

Dampak Pada e-comerce

Penggunaan aplikasi e-commerce dipengaruhi oleh tindakan Cybercrime. Munculnya kerugian bagi pengguna, mengurangi kepercayaan pengguna pada e-commerce, memberikan tambahan kunci keamanan yang merepotkan, membutuhkan perlindungan hukum yang tinggi bagi pengguna merupakan indikator dalam e- commerce karena adanya tindak Cybercrime. Banyaknya kerugian yang menimpa pengguna ecommerce akibat adanya Cybercrime berdasarkan hasil penelitian sangat mempengaruhi penggunaan ecommerce oleh pengguna di kemudian hari. Cybercrime sangat merugikan pengguna seperti kehilangan banyak waktu, kehilangan finansial, atau kehilangan data. Hal ini ditanggapi oleh responden dengan skor 86,2%. Kepercayaan pengguna pada e-commerce akibat kejahatan ini menurun. Tanggapan responden dengan skor 73,8% menunjukkan bahwa pengguna e-commerce tidak memberikan kepercayaan pada ecommerce. [6]

Dampak Pada Perbankan

Hasil penelitian ini mengindikasi bahwa lembaga keuangan mengandung risiko kejahatan
yang lebih tinggi dibanding lembaga lain. Semakin banyak nasabah yang memanfaatkan fasilitas internet banking dapat memberikan kesempatan bagi pelaku cyber crime untuk melakukan kejahatan kepada nasabah. Mengingat era saat adalah era digital, sehingga semakin banyak orang yang memanfaatkan keahliannya dalam menggunakan teknologi dan tidak sedikit dari mereka yang justru menyalahgunakan teknologi tersebut.[7]

Dampak Cyber Crime

Kurangnya pengawasan terhadap penggunaan internet menciptakan terjadinya kejahatan dunia maya. Kejahatan ini menggunakan akses internet yang tidak hanya terjadi dalam suatu wilayah. Keterbatasan Tenaga Ahli dalam melakukan penyelidikan menjadi faktor yang mempengaruhi keberhasilan aparat kepolisian dalam memberantas kasus cybercrime, dengan jumlah anggota ahli yang sangat minim menjadi batu hambatan dalam memberantas kasus kejahatan dunia maya yang tidak bisa diselesaikan dengan waktu yang efisien, sehingga hal tersebut dimanfaatkan oleh para pelaku dalam menjalankan aksinya dengan lebih leluasa. Personil[8]

Dampak kejahatan dunia maya bisa bermacam-macam. Pertama-tama, korban dapat berupa pengguna (orang atau organisasi) atau sistem komputer. Kedua, masing-masing dapat dipengaruhi dengan cara yang sangat berbeda, dari kerusakan yang tidak terdeteksi hingga kerugian finansial yang besar dan bahkan ada efek halus dan tidak berwujud pada individu (seperti menanamkan rasa takut terhadap dunia maya). Kekhawatiran tentang kejahatan dunia maya yang meluas telah ditanggapi dengan strategi global. Ini dibuat oleh negara-negara untuk membangun komitmen internasional untuk mewaspadai kejahatan dunia maya, mendorong perumusan aturan hukum untuk memerangi kejahatan dunia maya, membangun kerja sama internasional untuk memerangi kejahatan dunia maya, dan melakukan strategi non-alasan untuk menangani kejahatan

dunia maya. Dalam implementasinya, PBB telah membuat beberapa perjanjian yang mencakup kejahatan di dunia maya.[9]

Dalam perspektif kriminologi, penipuan identitas melalui duplikasi KTP konvensional dapat menjadi pintu masuk seseorang untuk melakukan kejahatan berulang. adanya identitas ganda tentu menjadi masalah yang dapat menghancurkan tatanan kehidupan masyarakat karena berpotensi melahirkan anak berulang. penjahat atau residivis.[9]

Salah satu masalah kejahatan dunia maya adalah pornografi dunia maya (khususnya anak pornografi) dan seks siber. Neill Barrett menegaskan bahwa pornografi dunia maya adalah salah satunya kejahatan yang terjadi di dunia maya yaitu kegiatan loading, accessing atau menyebarkan konten pornografi di media internet.Masalah ini juga mendapat perhatian serius dari dunia internasional, yaitu dengan kehadirannya dariKongres Dunia Pertama Menentang Eksploitasi Seksual Komersial Anak, Stockholm,27 – 31 Agustus 1996 danKonferensi Internasional tentang "Memerangi Pornografi Anak di Internet", mereka. Berdasarkan teori imitasi, media dapat membuat khalayak melakukan peniruan seperti yang disajikan, maka anak-anak atau remaja yang belum mampu menganalisis baik dan buruk melalui pikirannya, akan cenderung meniru dan mencoba apa yang baru dilihatnya. Akibatnya terjadi penyimpangan seksual, seperti masturbasi karena tidak ada tempat penyaluran atau bahkan bisa terjadi sebelum menikah dan hamil di luar nikah. Selain menyebabkan penyimpangan seksual, cyberporn juga dapat mengganggu perkembangan pribadi, seperti berkhayal atau berkhayal, malas bekerja, hingga kehilangan orientasi masa depan.[10].

Kesimpulan

Cyber Crime adalah akses illegal atau kejahatan dunia maya yang menggunakan computer sebagai sasaran atau objek utama dalam melakukan pencurian data jaringan dan pembobolan situs. Kejahatan yang menjadikan sistem teknologi informasi sebagai sarana pencurian data pribadi, pembuatan atau penyebaran virus, pembobolan sirus dan website.

Daftar Rujukan

[1] J. Studi and H. Pidana, "LS Cyber Crime dalam Instrumen Hukum Internasional :," vol. 5, no. 1, pp. 63–74, 2020.

[2] W. G. Kruse and J. G. Heiser, *Computer forensics : incident response essentials*. Addison-Wesley, 2001.

[3] H. Saini and Y. S. Rao, "Kejahatan Dunia Maya dan Dampaknya: Sebuah Tinjauan LIHAT PROFIL LIHAT PROFIL." [Online]. Available: www.onlinedoctranslator.com.

[4] A. W. Laksana, "PEMIDANAAN CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA POSITIF," 2019.

[5] L. Penelitian, "Kejahatan dunia maya: SEBUAHpeninjauan bukti," 2013. [Online]. Available: www.onlinedoctranslator.com.

[6] S. K. Rahayu, S. Ruqoyah, S. Berliana, S. B. Pratiwi, and H. Saputra, "Cybercrime dan dampaknya pada teknologi e-commerce," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 5, no. 3, p. 632, Aug. 2021, doi: 10.52362/jisamar.v5i3.478.

[7] N. R. Arofah, Y. Priatnasari, O. : Nida, and R. Arofah, "INTERNET BANKING DAN CYBER CRIME : SEBUAH STUDI KASUS DI PERBANKAN NASIONAL INTERNET BANKING AND CYBER CRIME: A CASE STUDY IN NATIONAL BANKING," 2020.

[8] Y. Prianto, N. A. Fuzain, and A. Farhan, "Seminar Nasional Hasil Penelitian dan Pengabdian Kepada Masyarakat 2021 Pengembangan Ekonomi Bangsa Melalui Inovasi Digital Hasil Penelitian dan Pengabdian Kepada Masyarakat Jakarta," 2021.

[9] R. Hukum, D. Global, P. Jurnal, and H. Jilid, "Dewi Bunga *," no. 51, pp. 69–89, 2019.

[10] H. Djanggih, "the Phenomenon of Cyber Crimes Which Impact Children As Victims in Indonesia," *Yuridika*, vol. 33, no. 2, p. 212, 2018, doi: 10.20473/ydk.v33i2.7536.

[11] Dessy,Sardy. 2013. Hubungan Penggunaan Media Sosial dengan Tingkat Pengetahuan Kesehatan Reproduksi Remaja Di SMAN 7 Jombang. Program Studi IV STIKES Jombang

[12] DeVito. Joseph A. 2001. The Interpersonal Communication. Book (9th ed) Addison Wesley Longman.
[13] Geçer, A. Kolburan. and Gü mü s .Aynur Eren. 2010. *Prediction of public and private university students*‟ communication apprehension with lecturers. *Procedia Social and Behavioral Sciences* 2: 3008–3014
[14] Errissya, Rasywir. 2015. Eksperimen Pada Sistem Klasifikasi Informasi Hoax Barbahasa Indonesia Berbasis Pembelajaran Mesin. *Jurnal Cybermatika* Vol. 3 No. Institut Teknologi Bandung
[15] Hidayat, Dedy N. 2008. Dikotomi Kualitatif – Kuantitatif dan Varian Paradigmatik dalam penelitian Kualitatif. *Jurnal Ilmiah SCRIPTURA*, Vol. 2 No.2 Juli 2008 Hal 81-94 http://download.portalgaruda.org/article.php?article=4150&val=358