Syntax Idea: p–ISSN: 2684-6853 e-ISSN: 2684-883X
Vol. 4, No. 9, September 2022

ANALISIS MODUS OPERANDI TINDAK KEJAHATAN MENGGUNAKAN TEKNIK KOMUNIKASI LOVE SCAM SEBAGAI ANCAMAN PADA KEAMANAN SISTEM INFORMASI

Ervan Yudi Widyarto, Dita Kusuma Hapsari
Politeknik Jakarta Internasional, Jakarta, Indonesia
Email: ervan.widyarto@jihs.ac.id, dita.hapsari@jihs.ac.id

Abstrak

Perkembangan teknologi informasi dan komunikasi yang semakin marak di dunia saat ini, memunculkan fenomena baru yang disebut kejahatan dunia maya (cybercrime), bahkan dapat juga dilakukan alih-alih komunikasi melalui love scam atau scammer love. Dalam penelitian ini kami ingin menyimpulkan beberapa faktor yang dapat menyebabkan terjadinya kejahatan dengan teknik komunikasi love scam untuk memberikan solusinya. Fenomena love scam atau scammer love. Aksi ini merupakan tindakan penipuan berkedok asmara. Biasanya pelaku memakai trik atau alih-alih kepercayaan yang melibatkan emosi atau perasaan si korban kemudian memanfaatkan perasaan atau niat baik itu untuk melakukan penipuan Jika dilihat dari dunia internet (Interconnected Network) tentang perbedaan gender, usia, bangsa dan penampilan fisik tidak menjadi soal, karena memang hal tersebut tidak bisa dilihat langsung. Itulah yang menyebabkan hacker tertarik untuk menggunakan Internet sebagai media komunikasi dan sekaligus membentuk sebuah komunitas, lantaran Internet cara paling cepat para hacker beraksi dan berinteraksi dengan si korban tanpa harus menunjukkan jati diri sebenarnya.

Kata Kunci: Interaksionisme Simbolik; Pemrosesan Informasi Sosial; Rekayasa Sosial; Komodifikasi Cinta; Seni Meretas; Mengeksploitasi

Abstract

The development of information and communication technology that is increasingly widespread in today's world, has led to a new phenomenon called cybercrime, it can even be done instead of communication through love scams or scammer love. In this study, we would like to conclude several factors that can lead to crime using love scam communication techniques to provide a solution. The phenomenon of love scam or scammer love. This action is an act of fraud under the guise of romance. Usually the perpetrator uses tricks or instead of trust that involves the emotions or feelings of the victim and then takes advantage of those feelings or good intentions to commit fraud. indeed it can not be seen directly. That's what causes hackers to be interested in using the Internet as a medium of communication and at the same time forming a community, because the Internet is the fastest way for hackers to act and interact with victims without having to show their true identity.

Keywords: *Symbolic Interactionism; Social Information Processing; Social Engineering; Commodification of Love; The Art of Hacking; Exploit*

How to cite:	Widyarto, E. Y. Hapsari, D. K. (2022). Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman pada Keamanan Sistem Informasi. *Jurnal Syntax Idea 4* (9) https://doi.org/10.36418/syntax-idea.v4i9.1959
E-ISSN:	2684-883X
Published by:	Ridwan Institute

Pendahuluan

Dalam teknologi informasi yang berkembang pesat di era globalisasi mengalami kemajuan dalam berbagai aspek sosial (Setiawan, 2018) Berdasarkan hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia tahun 2019 sampai tahun 2020 oleh Asosiasi Pengguna Jasa Internet Indonesia (APJII) bahwa 73,7 persen atau sekitar 196,71 juta jiwa dari penduduk Indonesia menggunakan internet diantaranya terdapat 12,2 persen sering menggunakan media sosial. Teknologi informasi saat ini seperti pedang tajam bermata dua, karena selain memberikan kontribusi pada perubahan sosial, kemajuan dan peradaban manusia, teknologi informasi juga digunakan sebagai wadah atau sarana untuk melakukan perbuatan melawan hukum (Ruslim, 2006). Tindakan melawan hukum seperti melakukan perusakan pada situs web, pencurian data pribadi pada jaringan sosial, dan penipuan yang disebut deception ditujukan untuk mencari dan mendapatkan keuntungan pribadi (Sulisrudatin, 2018)

Sutanto menjelaskan bahwa "suatu tindak kejahatan merupakan gambaran dari masyarakat. (Dewi, Wuryaningsih, & Susanto, 2020) Artinya kejahatan yang terjadi tidak terlepas dari lingkungan masyarakat itu sendiri" Bagi masayarakat awam, internet merupakan sebuah teknologi baru yang mampu membantu dan meringankan pekerjaan seperti tugas tugas sekolah, kampus, mencari data atasan, berkirim email, membaca berita, dan lain-lain. Aneka kemudahan ini meningkatkan rasa ingin tahu untuk berlama-lama di depan monitor komputer. Banyak sekali fasilitas yang membuat seseorang menjadi betah di depan komputer menggunakan internet, mulai dari chatting, milis, browsing, ditambah aplikasi canggih seperti video conference yang sudah mulai digunakan di seluruh dunia (Sawitri, 2020)

Pengguna internet bukan hanya sekadar menikmati kecanggihan fitur komunikasi saja, namun ada sebagian kalangan yang termotivasi untuk melakukan beragam hal yang tidak mungkin dilakukan di dunia maya (Faiza & Firda, 2018) Mulai dari menerobos sistem keamanan, membuka situs porno, melakukan porno aksi dengan webcam, chat sex dan lain-lain. Kebebasan untuk menjadi apa saja dan siapa saja membuat internet disukai banyak orang. Mereka berkepribadian tertutup atau pendiam, bisa berkompensasi jadi pribadi yang aktif di ruang chat atau milis (Zubaidah, 2022) Sehingga banyak sekali celah yang bisa diterobos tersebut, dari sisi karakter juga dari aplikasi. Komponen Keamanan Sistem. Prinsip dasar Keamanan Sistem Informasi. (Sari et al., 2020) Keamanan informasi (information security) adalah proses dan metodologi yang dibuat untuk melindungi informasi dan data penting dari aksespenggunaan, modifikasi dan pengerusakan yang illegal, serta penyalahgunaan, kebocoran data dan gangguan lainnya. Prinsip dasar dari keamanan sistem informasi adalah untuk melindungi kerahasiaan (confidentiality), ketersediaan (availability) dan integritas (integrity) data (Agustina & Kurniati, 2015)

A. Kerahasiaan *(confidentiality)*. Merupakan upaya perlindungan agar informasi tidak terakses oleh pihak yang tidak berwenang.

B. Ketersediaan *(availability)*. Prinsip ini berarti informasi selalu tersedia ketika dibutuhkan bagi orang-orang yang memiliki izin terhadap informasi tersebut.

C. Integritas *(integrity)*. Integrity merupakan proteksi informasi agar tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak diizinkan.

D. Pilar Keamanan Sistem Informasi

Menurut Amanda Andress seorang Analisis lembaga intelijen Amerika Serikat menyebutkan bahwa, ada tiga pilar dalam keamanan sistem informasi, yaitu: manusia, proses, dan teknologi.

Suatu sistem keamanan dibangun dengan menggunakan dokumen resmi perusahaan yang berupa standar, prosedur, maupun kebijakan. (Rafizan, 2011) Kebijakan yang dimiliki oleh perusahaan inilah yang akan menjadi landasan utama dalam keamanan informasi, dimana kebijakan tentang keamanan informasi sebaiknya harus ditandatangani oleh pimpinan puncak dari suatu perusahaan. Dengan adanya penandatanganan dari pimpinan puncak akan menandakan bahwa pimpinan sudah menyetujui adanya kebijakan tersebut dan menjadikannya sebagai prioritas utama dari perusahaan yang harus diikuti oleh semua karyawan perusahaan tersebut. Karena itulah dalam keamanan informasi, (Rafizan, 2011) suatu kebijakan menjadi urutan pertama yang harus diprioritaskan.

E. Manusia

Sebuah sistem dijalankan oleh manusia sebagai penggunanya, akan tetapi seperti yang dikemukakan oleh Prof. Richardus Eko lnd.rajit, dalam sebuah jaringan keamanan manusia menjadi bagian terlemah dalam sistem tersebut. Oleh karena itulah dalam keamanan informasi, manusia menjadi prioritas kedua yang harus diperhatikan.

F. Teknologi

Aspek teknologi digunakan untuk keamanan jaringan berupa penyettingan firewall , anti-virus, anti-spam, Intrusion Detection System (IDS) untuk mendeteksi keanehan di dalam jaringan, maupun Intrusion Prevention System (IPS) sebagai pencegahan jika ada terjadi penyerangan terhadap jaringan suatu perusahaan. Ketiga aspek tersebut menjadi sebuah kesatuan yang sangat penting dalam membangun keamanan informasi di dalam sebuah jaringan yang dimiliki oleh perusahaan, dimana aspek satu dengan yang lainnya saling mendukung.

G. Karakter Penjahat Digital

Cyber crime atau kejahatan siber dapat diartikan sebagai perbuatan melawan hukum yang dilakukan dengan komputer sebagai sarana atau alat, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Pada umumnya profil penjahat siber dimulai dari motivasi iseng setelah melihat adanya kesempatan, muncul niat untuk menerobos sistem keamanan kemudian mulai termotivasi dengan adanya mendapatkan keuntungan keuangan yang sangat besar. Kadang penjahat siber kelas atas didukung oleh suatu negara tertentu atau sekelompok politik radikal tertentu yang memiliki dana sangat besar dan tidak terbatas. Profil para penjahat cyber antara lain , sbb:

1. Karyawan yang tidak puas
2. Remaja
3. Hacktivis Politik
4. Peretas Profesional
5. Saingan Bisnis
6. Mantan/Keluarga Broken Home

Dunia kejahatan siber akrab dengan istilah hacker dan cracker. Hacker adalah orang yang ingin mengetahui lebih dalam terkait informasi-informasi penting milik individu atau organisasi (Idik Saeful Bahri, 2020).

Cukup mengejutkan bahwa Kementerian Komunikasi dan Informasi (Kemkominfo) memberikan informasi bahwa pengguna internet di Indonesia sudah mencapai angka 150 juta jiwa data dari APJII (Asosiasi Penyelenggara Jasa Internet). Keberadaan hacker ini tidak lain dipengaruhi oleh kegiatan pemerintah yang ingin mengembangkan internet di Indonesia. Namun sayangnya internet tersebut disalahgunakan oleh sebagian besar masyarakat sehingga dengan adanya internet dapat memicu perkembangan hacker/

Berikut ini adalah pengelompokan para hacker yaitu :

- Hacker Topi Hijau : Pemula
- Hacker Topi Putih : White hat hacker adalah hacker yang menjunjung tinggi standaretika dan hukum. Hacker Baik
- Hacker Topi Biru : Bertindak mencari celah sistem, lalu kerjasama dengan Developer agar segera diperbaiki. Hacker Baik
- Hacker Topi Merah : Seperti white hacker tapi lebih agresif. Tidak hanya mendeteksi kerentanan dan bertahan, tapi mengalahkan peretas. Hacker baik yang agresif.
- Hacker Topi Abu - abu : Hacker labil , kadang jahat atau baik tidak jelas arah hidupnya. Biasanya disebut dengan julukan Anti Hero, setia kepada yang memberikan penawaran paling menarik.
- Hacker Topi Hitam : Hacker Jahat. Nama lainnya adalah cracker orang yang sengaja merusak sistem keamanan, biasanya melakukan “pencurian” dan tindakan anarki. Motif Kejahatan.
- Cybercrime merupakan kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi dan terjadi di dunia cyber. Motif dari Cybercrime, yaitu:

a. Cybercrime sebagai tindak kejahatan murni. Dimana seseorang melakukan kejahatan secara sengaja dan terencana untuk melakukan tindakan anarkis, terhadap suatu sistem informasi atau sistem computer, baik itu pengrusakkan maupun pencurian data.
b. Cybercrime sebagai tindakan kejahatan abu-abu. Dimana kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.
c. 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/non materi.
d. Cybercrime yang menyerang Pemerintah. Kejahatan yang dilakukan dengan membajak ataupun merusak keamanan suatu lembaga pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahanatau menghancurkan suatu negara.
e. 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, dan lain-lain.

   Sedangkan berdasarkan jenis aktivitasnya, cybercrime dapat dibagi menjadi :

   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.

   2. llegal 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 contohnya pemuatan 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 melawanpemerintahan yang sah, dan sebagainya.

   3. Data Forgery
   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.

   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.

6. Offense against Intellectual Property
7. Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual (HAKI) 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.

Metode Penelitian

Peneliti menggunakan kerangka teori berfikir dari Antonio Gramsci. Metode prosedur penelitian ini adalah kualitatif dengan pendekatan etnografi. Penentuan informan dengan menggunakan cara purposive dan pengumpulan data dilakukan dengan pengamatan langsung, serta melakukan wawancara secara mendalam.

A. Komodifikasi Cinta.

Menurut Radita Gora dan Irwanto, maksud komodifikasi adalah komoditas yang diubah nilainya menjadi nilai tukar, digunakan pihak tertentu sebagai alat untuk mendapatkan keuntungan. Sehingga dapat diartikan dalam Komodifikasi Cinta merupakan pengubahan maksud dan makna cinta dengan memanfaatkannya menjadi jebakan atau peluang untuk mendapatkan keuntungan. Love scammers beraksi melakukan penipuan dengan berbagai cara untuk mendapatkan sejumlah besar uang dari korbannya yang mungkin awalnya tidak menyadarinya karena merasa telah mendapatkan cinta dan perhatiannya.

B. Strategi Kejahatan.

EC-Council, sebuah institusi terkemuka di dunia yang bergerak di bidang keamanan informasi dan internet membagi langkah--langkah yang dilakukan hacker dalam "beroperasi" menjadi 5 (lima) bagian yang berurutan satu dengan yang lainnya, yaitu: Banyak tehnik yang bisa digunakan oleh penjahat digital untuk mendapatkan informasi mengenai sasarannya. Langkah awal yang dilakukan yaitu dengan melakukan OSINT (Open Source Intelligence) mencari informasi di internet bisa berupa lokasi perusahaan, kondisi website, Struktur organisasi, List nama orang dalam organisasi, Tanggal ulang tahun, dan cara lainnya yang dapat digunakan nantinya untuk mengembangkan relasi/hubungan dengan targetnya. Phising Percobaan pertama yang dilakukan oleh penjahat digital untuk mendapatkan informasi yang sensitif, seperti data pribadi dengan menyamar sebagai seseorang yang mengagumi sang korban ingin mengenal lebih dekat melalui komunikasi elektronik resmi, seperti aplikasi chat yang telah di modifikasi mirip dengan tokoh fiktif. Pancingan dengan cara mengarahkan korban untuk bercerita maupun mengarahkan pembicaraan yang diperlukan agar semakin spesifik dan detail.

Spam Setelah Phising dilakukan langkah kedua Penjahat menyebarkan SPAM di internet atau perangkat komputer dan mobile. Tehnik SPAM dapat muncul di email, SMS dan Web. Bentuk dari SPAM ini merupakan iklan – iklan yang menggiurkan Korban untuk tergiur dengan iming – iming hadiah atau promo dimana content nya sudah disesuaikan dengan kesukaan atau Hobi sang korban data di dapat dari hasil Phising tujuannya sama agar korban dapat mengklik tautan yang telah disediakan berisi jebakan untuk mendapatkan data sensitif tersebut seperti data-data keuangan sang korban. Scam. Pada tahap ketiga ini penjahat akan mengirimkan sebuah email

yang nampaknya sangat meyakinkan tapi palsu kepada sang korban untuk mendapatkan data- data pelengkap agar tujuan aksi kejahatan nya dapat berjalan lancar.

Hasil dan Pembahasan

Tidak dipungkiri dan kita sadari bahwa wanita kebanyakan lemah ketika dihadapkan dengan masalah percintaan, apalagi ia tidak pernah diberi kelonggaran waktu oleh orang-orang di sekitar untuk berkenalan dengan seseorang pria diluar. Pikirannya hanya itu, memproteksi dirinya dari orang asing atau dia memiliki kepolosan hingga terbuai rayuan. Sehingga saat ditemui oleh seorang pria yang ia tidak kenal sama sekali dan sang pria itu mulai membual atau melakukan rayuan, sang wanita pasti akan terbawa emosi jatuh cinta, memberikan apa saja demi membuat sang pria merasa senang dan bahagia. Seperti yang terjadi pada studi kasus tersebut di atas, sang wanita terlalu polos untuk menanggapi sang pria yang belum pernah ia kenal sama sekali, sampai-sampai ia mau menjalin cinta dan juga bersedia memenuhi keinginan sang pria. Lalu, bagaimana selanjutnya? Apa yang bisa kita lakukan dan cegah dari kasus atau permasalahan tersebut? Jika tidak cepat ditangani, akan tambah banyak lagi korban *love scam* selanjutnya atau kasus lainnya (Kristanto, 2008).

Setelah melakukan penelitian secara menyeluruh mengenai aksi dari penjahat digital ini maka sangat diperlukan sebuah penanganan serius terhadap perlindungan data informasi. Akan sangat sulit jika kita hanya mengandalkan dari aspek teknologi semata untuk menutup masalah yang muncul, karena itu peran dari manusia sebagai pengguna sangat dibutuhkan untuk memperkuat sebuah sistim keamanan. Mulailah belajar sebagai pengguna yang MELEK digital, tidak mengabaikan informasi-informasi valid dan harus berpikir cerdas dalam menanggapi seseorang asing apalagi kita belum pernah bertemu dan hanya sebatas *chatting* saja. Seperti yang dikemukakan oleh Prof. Richardus Eko lndrajit, dalam ketiga aspek tersebut manusia menjadi bagian yang terlemah dalam sebuah jaringan keamanan. Manusia sebagai pengguna juga menjadi target utama bagi *Hacker*. *Social Engineering* berfokus pada mata rantai terlemah dalam rantai kemanan informasi-manusia. Kenyataannya, hampir semua solusi informasi sangat bergantung pada manusia. Kelemahan ini bersifat universal, dan terbebas dari *hardware, software, platform*, jaringan, dan usia peralatan. *Social Engineering* telah mencapai tingkatan tertinggi kematangan sebagai strategi dalam membobol keamanan informasi. Keamanan ini digunakan perusahaan untuk melindungi apa yang dianggap aset-aset paling penting perusahaan, termasuk informasi.

Mekanisme keamanan yang terbaik pun dapat ditembus dengan *social engineering*, untuk mengurangi resiko tersebut maka setiap organisasi dapat membantu menjamin keamanan dengan cara mengadakan program-program pelatihan kewaspadaan akan keamanan sistem informasi. Kewaspadaan diterapkan ke seluruh level yang paling bawah maupun manajemen level atas, mengenai ancaman keamanan dan bagaimana caranya mengenali serangan. Hal ini adalah kunci dari perlindungan berkelanjutan. Untuk dapat menggagalkan suatu serangan, akan lebih mudah jika kita mengenali serangan tersebut. Beberapa pertanda serangan *social engineering* yang dapat

dikenali antara lain menolak memberi kontak, terburu-buru, mencatut nama, intimidasi, hal-hal kecil seperti salah pengejaan nama atau pertanyaan agak aneh, dan meminta informasi terlarang. Saat dimana seorang pegawai merasakan adanya suatu keganjilan, dia memerlukan *prosedur* untuk melaporkan insiden yang terjadi. Sangat penting untuk adanya seseorang yang bertanggung jawab untuk melacak insiden-insiden ini. Selain itu pula, pegawai tersebut perlu memberitahu rekan-rekan kerjanya di posisi yang sama bahwa mereka pun mendapat ancaman serangan serupa.

Serangan *social engineering* terdiri dari aspek fisik dan aspek psikologis. Aspek fisik mencakup lokasi serangan seperti tempat kerja, telepon, mengacak-acak tong sampah, internet dan sebagainya (Thurlow, Crispin, Lengel, Laura, and Tomic, 2013). Sedangkan aspek psikologis mencakup segala sesuatu yang berkenaan dengan cara serangan itu terjadi seperti persuasi, menirukan orang, mencari muka, mencari kesamaan dan keramah-tamahan. Cara memerangi *social engineering* membutuhkan tindakan pada kedua aspek tersebut. Manajemen harus memahami pentingnya mengembangkan dan mengimplementasikan prosedur dan kebijakan keamanan sistem informasi yang baik (Griffin, 2006). Manajemen wajib untuk mengerti bahwa seluruh uang yang mereka habiskan untuk update perangkat lunak, perangkat keras kemanan, audit akan sia-sia tanpa persiapan yang cukup untuk menangkal *social engineering.*

Pencegahan Terhadap Serangan Fisik dilakukan dengan cara:

1. Pemeriksaan kartu identitas bagi siapapun yang memasuki gedung
2. Beberapa dokumen khusus perlu untuk dikunci dalam laci atau tempat penyimpanan aman.
3. Dokumen-dokumen lainnya perlu di shredding agar tidak bisa dibaca oleh pihak-pihak yang mungkin melakukan dumpster diving.
4. Media-media magnetik harus dihapus isinya agar datanya tidak bisa dipulihkan kembali.
5. Bila perlu, tong-tong sampah harus dikunci dan diawasi.
6. Semua perangkat yang terhubung dalam jaringan (termasuk sistem remote) perlu diproteksi dengan kata sandi (Sa'diyah, 2012)

Serangan psikologis dilakukan dengan cara merubah emosi seseorang sesuai dengan keinginan pelaku *social engineering* dengan cara melakukan persuasi, menirukan orang, mencari muka, mencari kesamaan dan keramah-tamahan.

Sebuah organisasi bisa berjalan dengan baik karena kedisiplinan pegawainya pada *Standard Operating Procedure (SOP)* yang telah ditetapkan. Bekerja diluar kewenangannya berpotensi fraud (Manthovani, n.d.2006)

Tujuan dari serangan psikologis adalah membuat pegawai perusahaan bekerja keluar dari SOP-nya, melakukan sesuatu diluar kewenangannya sesuai dengan keinginan pelaku *Social Engineering* (Manthovani, n.d. 2021)

Modus operandi terhadap kejahatan-kejahatan para *penjahat digital* disebut *Unauthorized Access to Computer System and Service,* yaitu melakukan suatu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Modus kriminalitas yang dilakukan *cracker*, salah satu bentuknya yang wajib diwaspadai adalah pencurian data-data *account*

penting. Pelaku biasanya adalah seorang *cracker* dengan cara menjebak orang lain untuk tidak sadar bersedia memberikan data-data *account*-nya. Modus operandi *cracker* ini sangat berbeda dengan tindak kejahatan konvensional. Hal yang paling mencolokdari perbedaan tersebut antara lain adalah terletak pada tempat kejahatan perkara karena dalam kejahatan ini yang diserang adalah jaringan komputer atau internet (Mansur, 2005).

Kesimpulan

Salah satu pemikiran yang salah, jika seseorang bahkan masih sebagian masyarakat Indonesia beranggapan bahwa sistem keamanan informasi merupakan hal yang biasa saja atau tidak penting. Ada juga masyarakat yang berpikir dan berkata bahwa, "pemerintah ribet, semua pakai digital" tanpa mereka berpikir panjang, padahal hal-hal seperti itulah sangat penting untuk mencegah peretasan dari *hacker*. Disinilah peranan pemerintah harus lebih aware dan siap siaga, mereka harus mencari dan memperhatikan seorang staff ahli yang khusus menangani sistem keamanan jaringan di suatu perusahaan untuk menutup akses atau kelemahan-kelemahan yang ada di sistem mereka, juga memperhatikan tata kelola IT secara menyeluruh agar dapat mengurangi, menghindari serta mencegah terjadinya suatu insiden pencurian data. Namun, peranan pengguna dan masyarakat melalui lingkungan, baik itu sekolah, kampus universitas atau penyambung perusahaan bisa dijadikan alat, media informasi dalam mensosialisasikan sistem keamanan informasi kepada seluruh khalayak luas agar bisa dibatasi dan mencegah *hacker* masuk ketika jaringan server sedang melemah.

BIBLIOGRAFI

Agustina, Esti Rahmawati, & Kurniati, Agus. (2015). Pemanfaatan kriptografi dalam mewujudkan keamanan informasi pada e-voting di indonesia. Seminar Nasional Informatika (SEMNASIF), 1(3).Google Scholar

Dewi, Erti Ikhtiarini, Wuryaningsih, Emi Wuri, & Susanto, Tantut. (2020). Stigma Against People with Severe Mental Disorder (PSMD) with Confinement "Pemasungan." NurseLine Journal, 4(2), 131–138. Google Scholar

Faiza, Arum, & Firda, Sabila J. (2018). Arus metamorfosa milenial. Penerbit Ernest.

Gora, Radita. (2015). Hukum, Etika, dan Kebijakan Media (Regulasi, Praktik, dan Teori). Deepublish. Google Scholar

Griffin, E. M. (2006). A first look at communication theory. McGraw-hill. Google Scholar

Idik Saeful Bahri, S. H. (2020). Cyber Crime Dalam Sorotan Hukum Pidana (Vol. 159). Bahasa Rakyat. Google Scholar

Kristanto, A. (2008). Jadi Hacker Siapa Takut. Yogyakarta: Universitas Atma Jaya Yogyakarta. Google Scholar

Mansur, Dikdik M. Arief. (2005). Cyber Law: Aspek Hukum Teknologi Informasi. Tiga Serangkai. Google Scholar

Manthovani, Reda. (n.d.). Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia, Jakarta: Malibu. Google Scholar

Rafizan, Onny. (2011). Analisis Penyerangan Social Engineering. Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 2(2), 115–126. Google Scholar

Ruslim, Harianto. (2006). HACK ATTACK: Konsep, Penerapan dan Pencegahan. Jakarta: Jasakom. Dapat dijumpai dalam situs internet: http://www. jasakom. Google Scholar

Sa'diyah, Nur Khalimatus. (2012). Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik. Perspektif, 17(2), 78–89. Google Scholar

Sari, Ika Yusnita, Muttaqin, Muttaqin, Jamaludin, Jamaludin, Simarmata, Janner, Rahman, M. Arif, Iskandar, Akbar, Pakpahan, Andrew Fernando, Abdul Karim, Sugianto, Giap, Yo Ceng, & Hazriani, Hazriani. (2020). Keamanan Data dan Informasi. Yayasan Kita Menulis. Google Scholar

Savitry, Dinda Cipta. (n.d.). Respons Jerman Terhadap Amerika Serikat (AS) Terkait Pengungkapan Program Pengawasan Massal National Security Agency (Nsa) Tahun 2013-2014. FISIP UIN Jakarta. Google Scholar

Sawitri, Dara. (2020). Penggunaan google meet untuk work from home di era pandemi coronavirus disease 2019 (Covid-19). Prioritas: Jurnal Pengabdian Kepada Masyarakat, 2(01), 13–21. Google Scholar

Setiawan, Daryanto. (2018). Dampak perkembangan teknologi informasi dan komunikasi terhadap budaya. JURNAL SIMBOLIKA: Research and Learning in Communication Study (E-Journal), 4(1), 62–72. Google Scholar

Sulisrudatin, Nunuk. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. Jurnal Ilmiah Hukum Dirgantara, 9(1). Google Scholar

Thurlow, Crispin, Lengel, Laura, and Tomic, Alice. (2013). Computer Mediated Communication: Google Scholar

Walther, Joseph B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. Communication Research, 23(1), 3–43. Google Scholar

Zubaidah, Zubaidah. (2022). Fantasi Introvert sebagai Ide dalam Lukisan. Institut Seni Indonesia Yogyakarta. Google Scholar