NETIZEN: JOURNAL OF SOCIETY AND BUSSINESS e-ISSN: 3032-4319
Vol. 1 No. 9 Agustus 2024, hal., 406-411

IMPLEMENTASI MANAJEMEN SECURITY TERHADAP CYBER CRIME DI INDONESIA

Rivaldi Rasqi Al Zahabi*[1], Sabni Gilang Permana[2], Angga wicaksana[3], Abdul Nasar[4], Fiqih Assidiq Ramadhan[5].
[1,2,3,4,5]Teknik Industri, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Bekasi Indonesia.
e-mail:*[1] 202210215034@mhs.ubharajaya.ac.id, [2] 202210215185@mhs.ubharajaya.ac.id,
[3] 202210215036@mhs.ubharajaya.ac.id, [4] 202210215021@mhs.ubharajaya.ac.id,
[5] 202210215027@mhs.ubharajaya.ac.id,
*Corresponding author : **Tubagus Hedi Saepudin**
e-mail : tubagus.hedi@dsn.ubharajaya.ac.id

Abstract

Cybercrime is a felonious act that utilizes computers or the Internet as its primary means of prosecution. InIndonesia, enterprises about cybercrime are raising, egging the government to introduce the Cybercrime Law. mindfulness ofdigital security pitfalls is also adding , especially regarding the vulnerability of particular information to abuse by reckless parties. This situation is aggravated by the lack of sweats to cover data in Indonesia, leading to a series of playing incidents and data breaches. These events include the hacking of social media accounts and identity theft, posing serious implicit impacts similar as particular data violations, highway robbery, and online fraud. The significance of regulations to guard particular data is decreasingly honored by the Indonesian government, as reflected in their sweats to draft and legislate Law Number 27 of 2022 on Cybercrime. This step demonstrates a serious commitment to gradationally enhancing the protection of particular data, with the stopgap of perfecting digital security and reducing the threat of cybercrime in Indonesia

Keywords : : *craking, identification, Cyber security..*

Abstrak

Kejahatan dunia maya (cybercrime) adalah tindakan keji yang memanfaatkan komputer atau Internet sebagai alat utama penuntutannya. Di Indonesia, perusahaan-perusahaan yang menangani kejahatan dunia maya semakin meningkat dan mendesak pemerintah untuk memperkenalkan Undang-Undang Kejahatan Dunia Maya. kewaspadaan terhadap kelemahan keamanan digital juga semakin meningkat, terutama mengenai kerentanan informasi tertentu terhadap penyalahgunaan oleh pihak-pihak yang ceroboh. Situasi ini diperparah dengan minimnya upaya untuk menutupi data di Indonesia, sehingga berujung pada serangkaian insiden perjudian dan pembobolan data. Peristiwa ini mencakup peretasan akun media sosial dan pencurian identitas, yang menimbulkan dampak implisit serius seperti pelanggaran data tertentu, perampokan di jalan raya, dan penipuan online. Pentingnya peraturan untuk menjaga data tertentu semakin tidak diapresiasi oleh pemerintah Indonesia,

sebagaimana tercermin dari upaya mereka untuk merancang dan membuat undang-undang Nomor 27 Tahun 2022 tentang Kejahatan Dunia Maya. Langkah ini menunjukkan komitmen serius untuk secara bertahap meningkatkan perlindungan data tertentu, sekaligus menyempurnakan keamanan digital dan mengurangi ancaman kejahatan dunia maya di Indonesia.
Kata Kunci: Cracking, Identifikasi, cyber security.

PENDAHULUAN

.Sebagai contoh, kejahatan dunia maya adalah menyebarkan data pribadi lewat jaringan ponsel.Warna-warni kejahatan yang dilakukan di dunia maya itu pada dasarnya menimbulkan dampak kusut dan bisa terpacu maraknya pengiriman barang tidak legal.maka para pelaku kejahatan dunia maya bisa dikalahkanl, dikurangi, namun termasuk juga di tangkap imajinatif.

Sebagaimana sebelumnya telah diulas bahwa manajemen keamanan, salah satu kegiatan yang terdiri atas dua kata, operasi -yaitu cubra lembar,ae atau lia- videlicet keamanan.2 merupakan‘ annoying kanca ’atau langkah pengerahan tenaga yang dilaksanakan melawan jebakan dan dilakukan mulai dari perencanaan, pengorganisasian, panegakan, pengawasan, sampai pengendalian. Dengan kata lain, aktivitas tersebut bertujuan untuk membantu dan mengurangi rugi akibakan jebakan yang digugat secara profesional dan odong-odong dirajut. Program keamanan siber, kesadaran pekerja aplikasi terhadap jebakan criminal siber, criminal siber peduli dan teknologi informasi, siber kesiapan Kominfo untuk menghadapinya adalah fokus eksplorasi mendalam peneliti.

sedikit demi sedikit, tantangan muncul seiring dengan semakin banyaknya data yang ditransfer dan disimpan secara elektronik, maka jalur pengamanan juga semakin rumit. Oleh karena itu, diperlukan analisis menyeluruh terhadap kendala-kendala yang akan terjadi, medan digital, dan hasil-hasil yang dapat diterapkan untuk meningkatkan keamanan siber. Studi tentang serangan yang telah terjadi dan cara mengatasinya sangat penting untuk memahami komplikasi dan tantangan yang terkait dengan menjaga objek dan garis penting. (Mahendra & Pinatih, 2023)

Banyak sekali kendala dan tantangan yang dihadapi oleh institusi pemerintah dalam penegakan pemerintahan khususnya di bidang keamanan informasi, antara lain sekuestrasi, integritas dan kekosongan data. Sehingga rencana tindakan e-Government juga harus memuat Sistem Manajemen Keamanan Informasi (ISMS), yaitu suatu rancangan suksesi untuk mengelola dan menjaga data yang benar-benar bersifat pribadi dan juga berarti bagi suatu kelompok/lembaga, yang baik pada basis pundi-pundi manusia. , Prosedur Standardisasi dan Sistem Teknologi Informasi.. tetap saja hal ini memerlukan tanggung jawab konsumen. Oleh karena itu, sangat penting untuk meningkatkan budaya keamanan siber sehingga masyarakat mempunyai

pemahaman untuk berbagi dan menyadari konsekuensi ketika menggunakan jaringan elektronik.(Aswandi et al., 2020)

METODE PENELITIAN

Jenis penelitian dalam eksplorasi ini adalah Sistem Eksplorasi Kualitatif dengan pendekatan deskriptif. Artinya, eksplorasi ini adalah tentang pengumpulan data dan mengujinya satu persatu dan suatu peristiwa atau fenomena itu tidak dapat dimonitrip sebagai komoditas saja seperti peristiwa terdahulu. Penulis ingin menerapkan gaya deskriptif kualitatif untuk menggambarkan hasil analisis mengenai seberapa operasional Manajemen Keamanan Terhadap Cyber Crime di KOMINFO. Para pelaku eksperimen menggunakan eksplorasi kualitatif untuk mengumpulkan data dengan mendalam, jelas, dan spesifik. Metode pengumpulan data menggunakan triangulasi, dan analisis data menggunakan induktif atau kualitatif. Desain eksplorasi ini menggunakan sistem deskriptif kualitatif karena penulis ingin mempermudah atau lebih mendeskripsikan kejahatan cyber.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi dan globalisasi ini telah membawa sebagian besar perubahan dalam kehidupan masyarakat. Dengan adanya bantuan dari teknologi informasi, komuikasi antara masyarakat dan negara menjadi jauh lebih mudah dan efektif, serta lebih mengefisienkan waktu, tanpa khawatir lagi akan sangat berguna sebagai sarana dalam membantu setiap negara dalam memberikan dua dampak yang menjadikan teknologi informasi berguna untuk memberikan sumbangan besar kepada pertumbuhan yang menguntungkan secara global. Langkah awal dalam teknologi informasi adalah untuk meningkatkan atau menaikkan permintaan terhadap suatu produk teknologi informasi itu sendiri. Tingginya permintaan terhadap layanan produk-produk tersebut sangat berdampak positif terhadap jalan pertumbuhannya ketekunan dalam teknologi informasi dan dapat mendorong penemuan. Langkah alternatifnya, dampak dari adanya teknologi informasi ini semakin memudahkan akses dalam dunia usaha, contohnya ada didalam bidang keuangan maupun kehidupan bisnis. Dari perkembangan teknologi informasi ini telah mengubah sebagian besar transaksi dalam dunia pembayaran dengan masuknya permintaan sistem pembayaran secara elektronik, perdagangan dengan sistem elektronik, dan layanan keuangan atau perbankan online.

Potensi dari ancaman terhadap *cyber crime* dapat berakibat pada perang *cyber*. Berikut adalah potensi ancaman kejahatan siber di Indonesia:

A. *Hacking* / Peretasan

kejahatan cyber mengacu pada aktivitas intrusif yang terkait dengan eksploitasi sistem komputer atau jaringan pribadi tanpa akses resmi.

B. *Cyber sabotage* / Sabotase dunia maya

Cyber sabotage / Sabotase dunia maya ini merupakan salah suatu perbuatan yang disengaja oleh para hacker untuk menghancurkan atau merusak suatu sistem informasi ataupun jaringan yang terhubung melalui Internet. Tindakan seperti ini dapat merugikan perusahaan bukan hanya secara sistem,tapi juga dapat merugikan secara fianansial perusahaan tersebut.

C. Identifikasi

Identifikasi adalah kemampuan untuk mengidentifikasi secara unik pengguna suatu sistem atau aplikasi yang berjalan di system. Identifikasi risko kejahatan dunia maya dilakukan secara rutin memberikan kemungkinan identifikasi akar masalah ketika menghasilkan dan memperoleh hasil yang akurat. Selama proses ini, semua yang menuju bisa menjadi penyebab kerusakan harus diidentifikas secara hati-hati. Setelah identifikasi lakukan, seluruh risiko yang dikenal diukur. Dua metrik kontrol Utama digunakan untuk mengukur kadar ancaman itu meliputi daftar antrian dan kerusakan.

D. Penilaian

Tujuan analisis risiko, hanya dapat dilakukan pada penilaian atas tingkat risiko pelanggaran dunia maya dan implikasinya pada berbagai bidang, termasuk pertahanan negara. Pada saat yang sama, tidak mungkin untuk secara langsung menilai beberapa tingkat risiko kriminalitas dunia maya. Analisis risiko kejahatan dunia maya didasarkan pada tabel matriks relatif. Dengan kata lain, pada penilaian risiko kriminalitas dunia maya dengan tabel matriks adalah perkiraan probabilitas dan impact dari ancaman kejahatan dunia maya yang dibedakan.

E. Merawat / *Treat*

Menghentikan tindakan dan melakukan tidakan penanggulangan resiko terkait kejahatan dunia maya yang meliputi keputusan apakah mentransfer, menerima, menghindarinya, ataupun meminimalkan. Dalam kasus ini di mana kejahatan seperti pencurian data dan informasi terjadi antara insitusi maupun individu, meminimalkan risiko kejahatan.

F. *Control*

Menilai efektivitas manajemen risiko, perbaikan berkelanjutan diperlukan dan pemantauan. Proses kontrol menyiratkan perlunya alat peringatan dini bagi fasilitor keamanan yang memiliki tanggung jawab, misalnya, Kementerian Pertahanan.

Untuk membangun pertahanan yang tak terkalahkan dalam dunia maya, perlu melibatkan teknologi canggih yang bisa memberikan dukungan dalam membangun sistem pertahanan negara maju dan modern. Sangat penting untuk

berkolaborasi agar mampu menghasilkan program . Ada dua faktor yang membantu meningkatkan sistem pertahanan ciber di Indonesia.

G. Spy device / Perangkat mata-mata

Sebuah program mengarah kepada perangkat lunak yang, tanpa izin pengguna, menggunakan jaringan untuk mentransfer informasi tentang, misalnya, cookie atau informasi. Informasi yang berhasil disimpan kemudian dapat dikirim atau dijual kepada perusahaan atau individu lain yang kemudian dapat menggunakan informasi itu untuk mengirimkan iklan yang tidak diinginkan atau bahkan menyebar virus berbahaya. Sayangnya, 24 infeksi malware terkait penggunaan perbankan online oleh masyarakat terdeteksi di Indonesia.(Putri et al., 2023)

Cyber-Security (Keamanan Siber)

Ada 3 contoh keamanan pada jaringan komputer pada cyber;

1. keamanan siber adalah kumpulan alat, program, generalisasi keamanan, perlindungan keamanan, pedoman, pendekatan operasi ancaman, perilaku, pelatihan, praktik gaya, jaminan, dan teknologi yang dapat digunakan untuk mencakup medan siber dan asosiasi serta sarana stoner yang disimpan dalam medan siber.
2. Keamanan komputer bertujuan untuk membantu para pengedar narkoba membantu penipuan atau mendeteksi upaya penipuan dalam sistem berbasis informasi. Informasi itu sendiri mempunyai makna non-fisik. Keamanan komputer adalah cabang teknologi yang dikenal sebagai keamanan informasi yang diterapkan pada komputer. Pretensi keamanan komputer mencakup menjaga informasi dari pencurian atau korupsi, atau menjaga kekosongan, sebagaimana diuraikan dalam kebijakan keamanan
3. Pengoperasian keamanan komputer dalam kehidupan sehari-hari berguna untuk menjaga pundi-pundi jaringan, dimodifikasi, diterobos berkepentingan. dapat dikaitkan dengan isu-isu khusus, terarah, hukum dan politik. Keamanan komputer akan menghilangkan 2 dampak penting, kesalahan besar dan dosa sistem.

Cyber-Crime (Kejahatan cyber)

kejahatan cyber merupakan kejahatan yang berhubungan dengan bias komputer atau jaringan, umumnya kejahatan ini dilakukan secara online. Sebenarnya kejahatan cyber ini bisa menyasar siapa . Namun, jelas akan menimbulkan banyak kerugian, jika Anda menjadi salah satu korbannya. Salah satu jenis kejahatan yang meningkat selama epidemi ini disebabkan oleh perubahan budaya online masyarakat. Ada beragam modus kejahatan dunia maya. Mulai dari pencurian data, peretasan akun, hingga meminta sumbangan atas nama korban epidemi.

Peran Cyber Security dan Ancaman nya

Keamanan cyber pada sebuah negara untuk menjaga data dan informasi.cyber security threat atau ancaman keamanan cyber mengacu pada kemungkinan tindakan atau serangan kejahatan yang berupaya mengakses data secara tidak sah, mengganggu operasi digital atau merusak informasi.(Indah et al., 2023) jenis – jenis ancaman pada cyber security yang harus kita waspadai:Ransomware, malware, phishing, spoofing, man in the middle.

KESIMPULAN DAN SARAN

Mencuri sebuah informasi dan data pribadi milik orang adalah kejahatan dunia yang menargetkan individu, perusahaan, dan data pemerintah di suatu negara. Kemenko polukan dan polri saling kerjasama untuk menjaga data masyarakat dan negara. kejahatan terhadap salah gunanya informasi di media sosial, dan berdampak pada masyarakat dan negara lain . Selain itu juga bisa melindung data pertahanan negara dari cyber. untuk menghadapi kejahatan pada siber perlu bantuan orang yang ahli dibidan cyber dan kerja sama antar pemerintah.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238.

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan data dan informasi pribadi melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*, 167–190.

Firmansyah, M., & Masrun, M. (2021). Esensi Perbedaan Metode Kualitatif Dan Kuantitatif. *Elastisitas: Jurnal Ekonomi Pembangunan*, *3*(2), 156–159.

Hilmy, M. I., & Azmi, R. H. N. (2021). Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lemhannas RI*, *9*(1), 114–124.

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 57–64.

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *6*(4), 1941–1949.

Putri, C. P., Anggraini, W., Hasibuan, Y. M., & Nurbaiti, N. (2023). Strategi Pengamanan Cyber: Lingkup Kerjasama dalam Menghadapi Ancaman Cyber. *INSOLOGI: Jurnal Sains Dan Teknologi*, *2*(6), 1124–1130.