
Mengatasi Ancaman Cyber Terhadap Privasi Data Pribadi

Anisa Puspita

anisapuspita613@gmail.com

Universitas Islam Negeri Sumatera Utara

Muhammad Irwan Padli Nasution

irwannst@uinsu.ac.id

Fakultas Ekonomi Dan Bisnis Islam, Prodi Manajemen,

Universitas Islam Negeri Sumatera Utara

Korespondensi penulis : *anisapuspita613@gmail.com*

Abstract: *Cyber threats to data privacy are a serious challenge for every individual in this digital era. Personal data protection and digital surveillance are important in dealing with this threat. In Indonesia, cyber security challenges involve a lack of public literacy, a lack of specific government policies, and a lack of competent human resources in the field of cyber security. The method used in this research is to collect articles that have been published in national publications and use a qualitative research approach. This paper discusses cyber threats.*

Keywords: cyber, privacy, defense

Absrak: Ancaman cyber terhadap privasi data merupakan tantangan serius bagi setiap individu pada era digital ini. Perlindungan data pribadi dan pengawasandigital menjadi penting dalam menghadapi ancaman ini. Di Indonesia, tantangan keamanan siber melibatkan kurangnya literasi masyarakat, minimnya kebijakan pemerintah yang spesifik, dan kekurangan sumber daya manusia yang kompeten dalam bidang keamanan siber. Metode yang digunakan pada penelitian ini adalah dengan menggumpulkan artikel-artikel yang telah dimuat pada publikasi nasional dan menggunakan pendekatan penelitian kualitatif. Paper ini membahas tentang ancaman cyber.

Kata kunci: cyber, privasi, tantangan

PENDAHULUAN

Era digital merupakan suatu zaman yang dimana kehidupan manusia menggunakan serba digital. Sebagai perkembangan lebih lanjut dari revolusi teknologi komunikasi, perang siber merupakan suatu keadaan konflik yang memanfaatkan perkembangan teknologi informasi dan komunikasi. Cyberwarfare merupakan fenomena sosial dalam hubungan internasional yang menimbulkan permasalahan serius dalam membangun stabilitas internasional di seluruh dunia.

Salah satu tantangan terbesar yang dihadapi era digital modern adalah ancaman cyber terhadap privasi data. Baik individu maupun bisnis lebih rentan terhadap serangan cyber yang mengakibatkan pelanggaran privasi dan hilangnya data penting. Oleh sebab itu, sangat penting untuk mengambil tindakan untuk melawan ancaman cyber ini guna menjaga keamanan data pribadi.

Di era digital, perkembangan teknologi informasi dan komunikasi telah banyak mengubah kehidupan masyarakat. Dalam perkembangannya data pribadi menjadi lebih

penting dan rentan banyaknya kegiatan yang dilakukan secara online. Data pribadi mencakup informasi seperti nama, alamat, dan informasi sensitif lainnya yang berkaitan dengan individu.

METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah dengan menggumpulkan artikel-artikel yang telah dimuat pada publikasi nasional dan menggunakan pendekatan penelitian kualitatif. Paper ini membahas tentang ancaman cyber.

HASIL DAN PEMBAHASAN

Pengertian Ancaman Cyber

Revolusi industri telah mempercepat perkembangan teknologi informasi dan komunikasi serta perubahan pada gaya hidup masyarakat di seluruh dunia. Erabaru ini disebut sebagai era digital atau era sistem siberfisik. Fenomena baru di bidang keamanan nasional dan internasional telah berkembang di era sistem siber-fisik ini: perang siber (cyberwar) dipandang sebagai tantangan atau ancaman pada abad ini. Di era sistem siber-fisik muncul fenomena baru dalam aspek keamanan nasional dan internasional yaitu perang siber yang dianggap sebagai tantangan maupun ancaman baru abad ini. Ancaman cyber mengacu pada peperangan yang dilakukan melalui dunia maya, dan karena dunia maya tidak terbatas, perang cybersangat mudah dilakukannya kapan saja, dimana saja. Karena teknologi komputer dan internet sering digunakan dalam perang cyber, sering terjadi persaingan antar pihak untuk mengontrol dan memanfaatkan informasi dan sumber daya teknologi yang tersedia. Perang siber (cyber war) seperti dijelaskan oleh Richard A. Clarke dan Robert K. Knake (2010, p. 11), adalah suatu tindakan dimana suatu negara membobol komputer dan jaringan yang ada di negara lain dengan tujuan untuk menimbulkan kerugian.

Pengawasan Data Privasi

Setiap informasi yang diproses oleh mesin yang berjalan secara otomatis sebagai respons terhadap arahan dan disimpan dengan tujuan untuk memprosesnya disebut sebagai data. Oleh karena itu, diperlukan peraturan perundang-undangan untuk memastikan bahwa data pribadi tidak disalahgunakan. Jerry Kang mendefinisikan data pribadi sebagai informasi yang terhubung langsung dengan seseorang dan membantu membedakan ciri-ciri uniknya. Secara umum, ada dua jenis perlindungan data:

perlindungan yang melibatkan pengamanan data berwujud, yang mencakup data yang terlihat dan tidak terlihat. Peraturan yang melarang penggunaan data oleh pihak yang bukan berwenang, menghubungkan data untuk tujuan tertentu, atau memusnahkan data sama sekali merupakan metode lain untuk melindungi data.

Menurut Warren dan Brandeis, “privasi adalah hak untuk menikmati hidup dan hak untuk dibiarkan sendiri, dan perkembangan hukum ini tidak dapat dihindari dan memerlukan pengakuan hukum.” Karena setiap orang mempunyai hak untuk menikmati privasinya, privasi tersebut harus dijaga.

Pemantauan Virtual Hubungan antara tindakan, perilaku, atau prosedur pembagian informasi dalam masyarakat dikenal sebagai pengawasan, dan sering kali dilakukan dengan tujuan untuk mempengaruhi, mengendalikan, membimbing, atau melindungi mereka yang terlibat. Pengawasan, seperti penyadapan, dilakukan dalam lingkungan digital dengan menggunakan teknologi dan jaringan digital

Tantangan Keamanan Siber Di Indonesia

Selama beberapa tahun terakhir, hambatan utama penerapan keamanan siber di Indonesia disebabkan oleh sejumlah alasan yang signifikan. Pertama, masih kurangnya kesadaran masyarakat Indonesia akan pentingnya keamanan siber bagi pengguna internet karena rendahnya tingkat literasi mereka (Maulia, 2017). Kedua, tidak adanya aturan eksplisit dari pemerintah mengenai keamanan informasi merupakan sebuah tantangan, terutama karena UU ITE memberikan penjelasan yang tidak jelas mengenai beberapa jenis ancaman siber di dunia kontemporer.

Selain sumber daya mentah, salah satu permasalahan keamanan siber terbesar di Indonesia adalah kurangnya sumber daya manusia (SDM) yang berkualitas dan berpengalaman. Hal ini disebabkan oleh dominasi spesialis asing di bidang keamanan siber, sehingga menghambat proses transfer teknologi yang diperlukan untuk menegakkan keamanan siber dengan baik.

Cara Menghindari Kejahatan Cyber

Untuk menghindari ancaman cyber, ada sejumlah tindakan proaktif yang dapat dilakukan. Yang pertama membuat kata sandi yang kuat untuk setiap akun dan menahan diri untuk tidak mengungkapkan informasi pribadi kepada publik di situs web seperti media sosial atau forum. Kedua, untuk bertahan dari serangan

malware dan peretas, instal aplikasi antivirus dan firewall tepercaya di PC dan perangkat seluler. Selanjutnya, demi perlindungan diri sendiri, selalu periksa ulang URL sebelum mengeklik tautan—ini sangat penting jika menerima email atau SMS aneh. Selanjutnya, gunakanlah jaringan WiFi yang aman juga dianjurkan, terutamasaat menangani data sensitif atau melakukan pembayaran. Berhati-hatilah terhadap pesan phishing yang meminta informasi pribadi, dan perbaharui perangkat lunak secara berkala atau teratur untuk menghilangkan kerentanan keamanan. Selanjutnya, dianjurkan untuk melakukan pemilihan dan pertimbangan untuk menggunakan layanan keamanan online. Terakhir, penting untuk memahami hak perlindungan data dan aturan privasi yang berlaku untuk layanan online yang digunakan agar dapat mengontrol dan melindungi data pribadi dengan lebih baik. Meskipun pemerintah Indonesia telah mengambil langkah-langkah untuk mengatasi masalah ini, hal ini masih menjadi tantangan bagi semua negara seiring kemajuan teknologi. Untuk menghentikan kejadian serupa di masa mendatang, sejumlah langkah dapat dilakukan. Menjaga perangkat lunak tetap diperbarui adalah salah satu pertahanan terbaik melawan peretas untuk sebuah situs web. Bisnis harus menggunakan HTTPS, menginstal plugin keamanan dan SSL, dan mengikuti pembaruan perangkat lunak keamanan. Berinvestasi dalam pencadangan otomatis juga penting. Selalu ada kemungkinan kehilangan segalanya karena peretasan situs web, bahkan setelah semua tindakan pencegahan lainnya diterapkan. Pencadangan informasi secara teratur dapat membantu mencegah hal ini. Sebuah situs web juga dapat diamankan dari peretas dengan berhati-hati saat mengizinkan pengunggahan file. Saat mengunggah konten ke situs web, pengguna mempunyai kemampuan untuk menyalahgunakan fitur ini dengan memuat file berbahaya.

KESIMPULAN

perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan dalam kehidupan masyarakat di era digital, termasuk munculnya ancaman cyber sebagai tantangan utama di abad ini. Ancaman ini meliputi perang siber, pengawasan digital, dan tantangan keamanan siber yang dihadapi oleh berbagai negara, termasuk Indonesia. Untuk menghindari kejahatan cyber, langkah-langkah preventif seperti menggunakan password yang kuat, menginstal program antivirus, memperbarui perangkat lunak, dan berinvestasi dalam keamanan situs web sangat diperlukan.

DAFTAR PUSTAKA

- Rima, K., & Sarjana, M. (2023). Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia. *Jurnal Analisis Hukum*, VOL. 6 NO 1.
Doi:<https://doi.org/10.38043/jah.v6i1.4484>.Retrived From
<https://journal.undiknas.ac.id/index.php/JAH/article/view/4484>
- Salmon A.M. Babys. (2021). Ancaman Perang Siber Di era Digital Dan Solusi Keamanan Nasional Indonesia. *Jurnal Oratio Directa*, VOL. 3 NO. 1. E- ISSN 2615-07435.Retrieved From
<http://ejurnal.ubk.ac.id/index.php/oratio/article/view/163/116>
- Citra, Y,. & Pinatih , N. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran*, VOL. 6 NO.Doi:<https://doi.org/10.31004/jrpp.v6i4.20659>.Retrieved From
<https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659>
- Na'im, M, (2018). Analisa Keamanan Dan Hukum Untuk Perlindungan DataPrivasi. *Cybersecurity Dan Forensik Digital*, VOL. 1 NO. 2 e-ISSN: 2615-8442.Retrieved From <https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/1370/1286>