Telecommunications, Networks, Electronics, and Computer Technologies

Vol.1 (2), 2021, 85-92

JURNAL UPI

TELNECT

Journal homepage: http://ejournal.upi.edu/index.php/TELNECT/

Ancaman dan Solusi Serangan Siber di Indonesia

Sahat Parulian[1], Devi Anassalifa Pratiwi[2], Meiliya Cahya Yustina[3]*

[1,2,3] Program Studi Sistem Telekomunikasi, Universitas Pendidikan Indonesia, Bandung, Indonesia

*Corresponding Author: E-mail: sahatparulian@upi.edu

ABSTRACTS

Sepanjang bulan januari sampai dengan juli 2021 tercatat 741.441.648 ancaman siber yang telah terjadi di Indonesia. Ancaman siber tersebut memiliki dampak yang sangat berbahaya bahkan potensi ancaman bagi pemilik akun yang diserang. Adapun tujuan dari penelitian ini adalah untuk mengetahui apa yang dimaksud dengan ancaman siber, menganalisis beberapa kasus-kasus yang sering berpotensi dengan penyerangan siber, apa saja faktor-faktor yang mempengaruhi terjadinya ancaman siber saat ini, seberapa besar pengaruh ancaman siber pada data pribadi, dan analisis bagaimana solusi pencegahan yang dapat dilakukan dalam menghadapi ancaman siber. Penelitian ini menggunakan pendekatan studi literatur dari sumber-sumber terpercaya dengan mengamati dan menganalisa berbagai kasus yang sedang terjadi saat ini. Berdasarkan hasil yang dillakukan penulis bahwa terjadi peningkatan ancaman siber sebesar 6,15% yang terjadi di Indonesia dari tahun 2020 s/d 2021, ancaman yang sering terjadi di antaranya serangan *Denial of Service (Dos) Attack* yang berupa serangan *synflood* dan ICMP *flood, phising,* serta pencurian data pribadi. Mitigasi yang dapat dilakukan dari ancaman siber antara lain tidak mudah termakan isu berita hoax, memastikan setiap informasi yang diberikan dari orang lain dan yang lainnya

ARTICLE INFO

Article History:
Received 15 Oktober 2021
Revised 22 November 2021
Accepted 11 Desember 2021
Available online 15 Desember 2021

Keyword:
Ancaman Cyber,
Kasus,
Faktor,
Solusi

1. INTRODUCTION

.

Pesatnya kemajuan jaringan internet umumnya memberikan begitu banyak manfaat bagi perkembangan teknologi informasi dan komunikasi, karena dapat mangembangkan inovasi dalam meningkatkan kemajuan pradaban manusia modern. Adanya perkembangan teknologi informasi dan komunikasi di era sekarang menyebabkan kita selalu bergantungan dengan kelebihan dan kemudahan teknologi yang ditawarkan. Teknologi *online* dapat memudahkan kita dalam melakukan aktivitas kegiatan sehari-hari bahkan jika dimanfaatkan dengan bijak maka dapat dijadikan sebagai sumber penghasilan. Berbagai macam teknologi informasi dan komunikasi yang sedang kita rasakan sekarang pemanfaatannya yaitu media sosial *online* seperti *WhatsApp, Instagram, Meta atau facebook,TikTok, Tokopedia* dan lain sebagainya. Namun adanya kemunculan teknologi *online* tersebut justru membawa kita harus lebih waspada dan berhati hati karena semakin tinggi pula resiko yang akan dihadapi terutama ancaman *cyber*.

Maraknya kasus ancaman *cyber* yang terjadi karena berbagai faktor salah satunya adalah semakin tingginya akses pengguna *online*. Banyaknya informasi data pribadi yang masuk dan lemahnya sistem keamanan pada teknologi *online* tersebut memudahkan penyerangan pencurian informasi data. Meningkatnya pemanfaatan teknologi internet justru juga menjadi tantangan baru dalam perlindungan data pribadi, terutama pada pengumpulan, pemanfaatan, dan penyebaran data pribadi seseorang. Ancaman yang sering terjadi adalah penipuan yang memanfaatkan celah penggunaan teknologi digital.

Mengutip data Badan Siber dan Sandi Negara (BSSN), Menteri Kominfo Jhonny G. Plate, mengungkapkan bahwa sepanjang bulan januari sampai dengan juli 2021 tercatat 741.441.648 ancaman siber yang telah terjadi di Indonesia. Berbagai tindakan kejahatan yang sering terjadi seperti *hacking, cracking*, kejahatan *carding* (*credit card fraud*), ATM *skimming*, *phishing* (*internet banking fraud*), *cybersquatting*, *malware* (*virus/bots/worm), terorisme*, *human trafficking*, pinjaman *online* [1]. Tindakan-tindakan tersebut dapat dengan mudah dilakukan dengan memanfaatkan jaringan internet dan kemajuan teknologi di era sekarang.

Berdasarkan jurnal *Satrio dan Widiatno 2021* menjelaskan bahwa terkait keamanan data Facebook dikenal dengan sejarah perlindungan data yang begitu buruk bagi privasi penggunanya. Kebobolan data Facebook selalu jadi topik hangat pada 5 tahun belakangan ini tak terkecuali di 2021. Pada jurnal tersebut mengungkapkan bahwa kebocoran data Facebook telah terjadi di bulan februari 2021 hingga mencapai jumlah 130.000 pengguna asal Indonesia [2]. Pada jurnal *Rahmawati, 2017* mengungkapkan juga bahwa pada tahun 2007-2008 terjadi serangan kejahatan siber dengan memanfaatkan *Distributed Denial of Service (DdoS)* [3]. Tindakan tersebut menyebabkan lumpuhnya aktivitas negara karena banyak sektor kritis yang diserang. Selain itu diungkap juga pada jurnal yang berjudul *"TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN - 2nd National Conference on Law"* Pada tanggal 17 April 2020 telah terjadi serangan peretas internasional yang berhasil meretas 91 juta akun pengguna Tokopedia. Data tersebut diperjual belikan oleh pelaku sebesar *USS$ 5.000* atau sekitar Rp.74.000.000 [4].

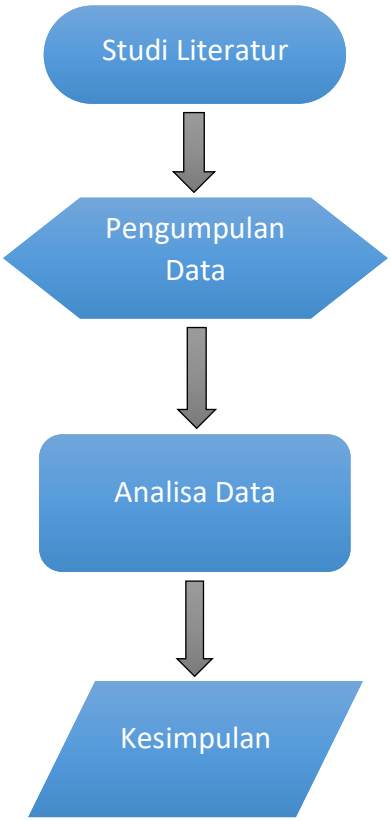
Berbagai penyerangan ancaman siber yang maraknya sering terjadi dikarenakan adanya kecerobohan dan lemahnya sistem keamanan teknologi *online* tersebut sehingga menyebabkan dampak yang sangat buruk bagi pemilik akun bahkan platform tersebut akan merasakan dampaknya pula. Berdasarkan publikasi *The Global Cybersecurity Index (GCI)* 2017 yang dirilis oleh *International Telecommunication Union (ITU),* kondisi keamanan siber Indonesia masih termasuk dalam negara dengan kategori keamanan siber yang lemah berada dalam tahap peningkatan optimal *(maturing stage)* [5].

Oleh karena itu, berdasarkan latar belakang berbagai kasus maraknya ancaman siber yang terjadi pada dunia internet dan perkembangan teknologi sekarang, maka pada penelitian ini penulis akan membahas apa saja faktor yang mempengaruhi terjadinya ancaman siber, seberapa besar pengaruh ancaman siber pada data pribadi, serta analisis bagaimana solusi pencegahan yang dapat dilakukan dalam menghadapi ancaman siber. Adapun hasil pengembangan yang dilakukan penulis dalam analisis penelitian ini adalah untuk mengetahui peningkatan ancaman siber pada tahun 2020 s.d. 2021 dan memberikan mitigasi terhadap ancaman siber yang terjadi di Indonesia.

2. MATERIALS AND METHODS

Metode pengumpulan data yang akan digunakan dalam penelitian ini untuk mengumpulkan data-data yang diperlukan oleh peneliti adalah Metode Studi Literatur. Metode studi literatur ini merupakan suatu metode pengumpulan data, baik itu dalam bentuk tulisan, gambar dan karangan dari sumber-sumber terpercaya seperti artikel, jurnal, laporan penelitian, internet, dan lainnya. Teknik studi literatur ini dilakukan agar mendapatkan teori-teori yang relevan terhadap permasalahan-permasalahan yang

dibahas dalam penelitian ini. Sehingga peneliti dapat menyelesaikan masalah yang diteliti dan menarik kesimpulan berdasarkan teori-teori tersebut. Langkah-langkah dalam metode studi literatur dapat dilihat pada **Gambar 1.**



Gambar 1. Flowchart dari metode penelitian

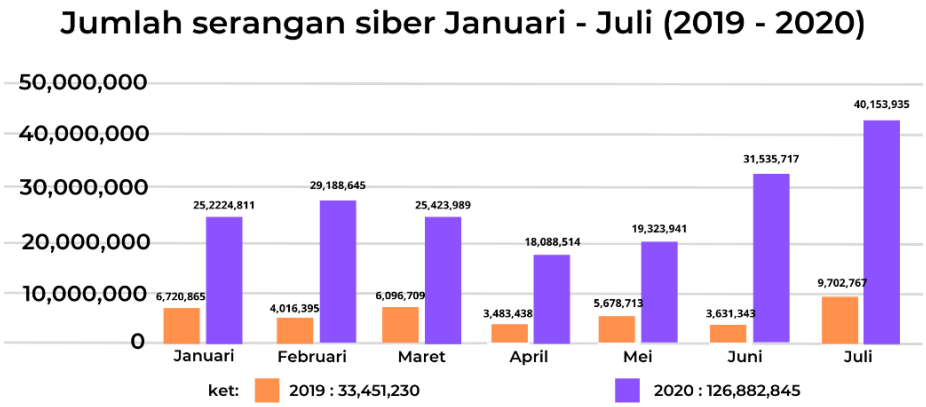
3. RESULTS AND DISCUSSION

Untuk mengetahui hasil dan diskusi yang peneliti lakukan dengan membaca beberapa literatur yang sudah dipersiapkan pada sebelumnya maka akan dipaparkan pada pembahasan berikut.

3.1 Results

Di era digital saat ini, ancaman siber semakin meningkat setiap harinya, bukan hanya di beberapa negara tetapi hampir seluruh dunia merasakan dampak dari adanya ancaman ini. Ancaman siber merupakan suatu tindakan kejahatan yang merusak, memanipulasi, dan mencuri suatu informasi penting dari sebuah aplikasi atau *website* yang meyebabkan masalah serius terhadap keamanan jaringan, database, atau sistem komputer.

Berdasarkan data yang diperoleh *kompas.com*[6] di Indonesia terdapat 33.451.230 ancaman siber yang terjadi pada bulan Januari – Juli 2019 dan sebanyak 126.882.845 di bulan Januari – Juli 2020, dari data tersebut dapat diperkiran ancaman siber mengalami peningkatan sebesar 9.35%. Selanjutnya, sejak awal tahun 2021 bulan januari hingga pertengahan tahun pada bulan Juli, terdapat 741.441.648 ancaman siber yang telah terjadi berdasarkan data yang di peroleh dari Badan Siber dan Sandi Negara (BSSN)[7]. Peningkatan ancaman siber yang terjadi pada tahun 2020 – 2021 mengalami peningkatan sebesar 6.15%. Data-data tersebut dapat dilihat pada **Gambar 2** dan **Gambar 3** [6].



Gambar 2. Jumlah serangan siber Januari - Juli 2019 s.d. 2020

Gambar 3. Jumlah serangan siber Januari - Juli 2021

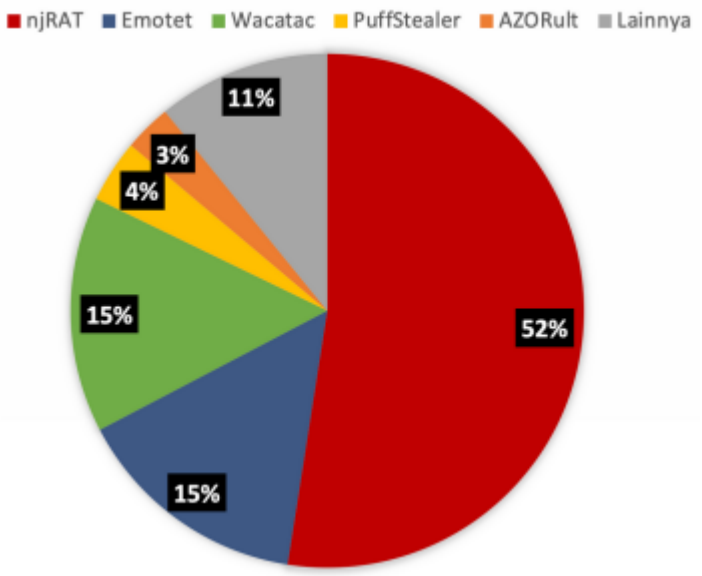
Berdasarkan data yang bersumber dari Jurnal yang berjudul "ANALISIS RUU TENTANG APBN – Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan"[8] mendapatkan bahwa anomali terbanyak Ancaman siber yang terjadi pada bulan Januari s.d. Juli 2020 adalah Penipuan *Online*, Penyebaran Konten Provokatif dan Pornografi.

TABEL 1. ANOMALI KEJAHATAN SIBER BULAN JANUARI - JULI 2020

No.	Jenis Kejahatan	Jumlah
1.	Penipuan Online	8.2 K
2.	Penyebaran Konten Provokatif	7 K
3.	Pornografi	1.5 K
4.	Akses Ilegal	1.2 K
5.	Pencurian Data / Identitas	0.8 K
6.	Peretasn Sistem Elektronik	0.5 K

Pada tahun 2021 ancaman siber terjadi pada sektor yang menargetkan pemerintahan, keuangan, penegakan hukum, telekomunikasi, transportasi dan perusahaan [7]. Jika dilihat dari **Gambar 3.** bahwa sektor pemerintahan yang sering terjadi penyerangan dan menjadi target utama para *attacker* atau *hacker, hacker* adalah seseorang yang memiliki *skill* dalam membobol atau merusak sistem keamanan operasi komputer yang memiliki tujuan tertentu, secara umum *hacker* dibagi menjadi dua jenis yaitu *black hat* dan *white hat*, black hat merupakan *hacker* yang bertujuan untuk melakukan tindak kejahatan

demi keuntungan pribadi atau kelompok sedangkan *white hat* merupakan *hacker* yang bertujuan untuk melakukan tindakan secara legal untuk membantu sebuah perusahaan, pemerintahan atau organisasi vital lainnya yang memiliki pengaruh besar bagi Negara [9]. Selain itu, berdasarkan hasil *research* Badan Siber Sandi Negara (BSSN)[10] Indonesia mengemukakan bahwa sepanjang tahun 2020 terdapat ancaman pencurian data menggunakan beberapa jenis *malware* yang terdiri dari 52% njRAT, 15% Emotet, 15% Wacatac, 4% PuffStealer, 3% AZORult, dan 11% jenis yang lainnya.



Gambar 4. Hasil *research* Badan Siber Sandi Negara (BSSN) Indonesia [2].

4. Discussion

Dari hasil studi literatur yang penulis analisa di dapatkan berbagai ancaman siber yang terjadi di Indonesia, di antaranya sebagai berikut ini.

4.1 Denial of Service (DoS) Attack

Ancaman siber yang pertama adalah *Denial Of Service (DoS) Attack* yaitu suatu serangan yang memberhentikan layanan sementara ataupun permanen pada sebuah server *website* atau aplikasi dengan cara menggunakan botnet yang dijalankan secara bersamaan dalam satu waktu, membanjiri permintaan *request server* agar tidak dapat terhubung, membanjiri pesan icmp pada server dengan mengirim paket-paket yang sudah rusak oleh sang *attacker* [11], serangan ini dapat menyebabkan kerugian bagi client atau user tidak dapat mengakses sebuah website atau aplikasi yang dituju, serangan DoS dapat berupa ICMP Flood dan SYN *Flood*.

Contoh kasus yang dikutip dari "Activity | Tantri | Student Blog" menjelaskan penyerangan terhadap website *kaskus* oleh komunitas YogyaFree, dengan cara mengirimkan *thread-thread* berupa paket-paket rusak terhadap server, yang mengakibatkan website tidak dapat di akses bagi administrator ataupun pengunjung website. Faktor terjadinya ancaman ini adalah karena terdapat celah pada server sehingga rentan diserang oleh pelaku.

Mitigasi yang tepat untuk mencegah terjadinya serangan DoS *attack* adalah menggunakan *hashing* kriptografi, server mengirimkan respons SYN-ACK-nya dengan nomor urut (seqno) yang dibuat dari alamat IP klien, nomor port, dan mungkin informasi pengenal unik lainnya. Ketika klien merespons, hash ini disertakan dalam paket ACK [12]. Server memverifikasi ACK, dan kemudian mengalokasikan memori untuk koneksi, selanjutnya menggunakan snort dengan rule yang sudah disiapkan dan akan dijalankan pada server, serta membatasi memproses pesan ICMP yang masuk [13].

4.2 Pencurian Data

Ancaman siber yang kedua adalah pencurian data dan informasi pribadi melalui internet, maraknya kasus tindak kejahatan ini sering terjadi karena lemahnya aturan yang berlaku dalam melindungi data pribadi. Berdasarkan publikasi *The Global Cybersecurity Index (GCI)* 2017 yang dirilis oleh *International Telecommunication Union (ITU),* kondisi keamanan siber Indonesia masih termasuk dalam negara

dengan kategori keamanan siber yang lemah berada dalam tahap peningkatan optimal *(maturing stage)* [5].

Selain itu pelaku ingin mengambil keuntungan bagi dirinya sendiri tanpa memikirkan orang lain dengan cara yang tidak halal, pencurian data dan informasi dapat dilakukan dengan cara membuat dan menyebarkan informasi *hoax* [14] dengan tujuan untuk menyulut sensasi pada media sosial atau justru dengan sengaja bertujuan supaya pengguna internet dapat terbawa untuk mengunjungi website pembuat berita Hoax tersebut demi meraup keuntungan dari tingginya jumlah *traffic* pada situs yang dikelolanya. Kemudian, salah satu aplikasi media sosial dengan banyaknya kasus informasi hoax adalah facebook terdapat 110 informasi hoax yang beredar pada tahun 2018, tidak hanya itu saja pencurian data pun terjadi pada aplikasi yang dibangun oleh *Mark Zuckerberg* ini, terdapat 87 juta data pribadi pengguna facebook diambil secara cuma-cuma oleh perusahaan *Cambridge Analytica* [15].

Pencurian tersebut terjadi akibat terdapat celah *pada Application Programming Interface (API)* yang digunakan oleh pengembang aplikasi pihak ketiga, tidak hanya itu saja, modus lain yang beraksi pada aplikasi *Facebook* adalah pelaku menyimpan virus atau malware pada sebuah postingan yang akan ditampilkan pada beranda *Facebook*, ketika korban mengklik postingan tersebut secara tidak langsung akan mendownload virus atau langsung diarahkan ke halaman tautan situs website yang berisi malware, sehingga pelaku akan dengan mudah mengendalikan *device* korban untuk mencari informasi mengenai data pribadi korban[16].

Mitigasi yang tepat agar tidak menjadi korban dari pencurian data pribadi dari media sosial seperti *facebook* atau yang lainnya adalah dengan memperkuat aturan perundang-undang mengenai pencurian data pribadi, meningkatkan kerja sama keamanan siber menjadi salah satu strategi yang dapat dilaksanakan pemerintah Indonesia diharapkan dalam menyelenggarakan kerja sama baik bilateral maupun multilateral terutama terkait bidang keamanan siber dengan negara lain. Kerja sama antara pemerintah dengan pihak swasta diharapkan dapat ditingkatkan guna mendorong pertumbuhan ekonomi dan teknologi keamanan siber. Pencegahan lain yang dapat dilakukan secara individu yaitu dengan mencari informasi lebih lanjut mengenai berita yang diberikan oleh orang yang tidak dikenal dalam menggunakan sosial media, kemudian tidak asal mengklik postingan yang bukan dari sumber terpercaya atau orang yang tidak dikenal, serta bijak dalam memilih dan memilah informasi yang beredar di media sosial[17]. Akibat dari pencurian data pribadi dapat menyebabkan kerugian yang cukup besar, salah satu contohnya adalah data pribadi tersebut dapat digunakan untuk pinjaman online illegal atau pembayaran kartu kredit[18].

4.3 Phising

Ancaman siber yang ketiga adalah beredarnya situs palsu atau phising yang bertebaran di internet. Phising merupakan tindakan kejahatan media sosial, dengan merekayasa atau mengelabui isi konten dari suatu website atau aplikasi [19], sesuai dengan yang aslinya, faktor dari terjadinya kejahatan ini adalah untuk meraup keuntungan pribadi secara ilegal dengan cara mendapatkan informasi pribadi mengenai alamat *email, username, password*, nomor kredit dari dan data penting lainnya dari sang korban. Kerugian dari ancaman siber ini yaitu pelaku dapat secara leluasa mengambil alih akun dari sang korban, akun tersebut dapat berupa kartu kredit, alat transaksi *online* seperti paypal, dana, ovo dan yang lainnya [20].

Salah satu contoh kasus aktivitas phising di Indonesia dikutip pada jurnal yang berjudul "Aktivitas Phising Sebagai Tindak Pidana Dalam UU ITE Repository - UNAIR REPOSITORY" menjelaskan kasus pembuatan sebuah situs palsu yang serupa dengan website *mobile banking* milik bank BRI oleh Suparman beserta rekannya Ikhsan, pelaku melakukan aktivitas tersebut dengan cara mengirimkan SMS caster kepada sejumlah orang yang memiliki rekening bri.

Mitigasi agar tidak tertipu oleh ancaman phising ini antara lain, memastikan nama pengirim *email* setiap kali ada pesan yang masuk melalui layanan penyedia email seperti *yahoo*, *gmail*, dan layanan penyedia yang lainnya, kemudian tidak asal klik link yang diberi oleh orang tidak kenal, selanjutnya memastikan keamanan website yang akan di akses dengan cara melihat alamat *website* yang dituju apakah menggunakan https atau http, jika https maka alamat *website* tersebut aman selain itu pastikan nama *website* yang dituju benar dan resmi, serta domain *website* yang dipakai secara umum dan legal menggunakan "com, edu, " atau "go.id" bagi negara Indonesia[21].

5. CONCLUSION

Dari penelitian yang dilakukan oleh penulis dapat disimpulkan bahwa di tahun 2019 s.d. 2021 pada bulan januari hingga juli ancaman siber mengalami peningkatan. Peningkatan ancaman siber yang terjadi di tahun 2019 – 2020 sebesar 9.35% dan di tahun 2020 – 2021 sebesar 6.15%. Beberapa ancaman siber yang terjadi di Indonesia, antara lain serangan *DoS* terhadap *website kaskus* oleh komunitas YogyaFree, pencurian data pribadi melalui halaman Facebook dengan menyebarkan berita hoax dan pembuatan situs phising *mobile banking oleh* suparman dengan rekannya ikhsan. Adapun faktor yang mempengaruhi dari terjadinya ancaman siber pada penelitian ini diantaranya yaitu untuk meraup keuntungan yang tinggi dari jumlah *traffic* pada situs hoax yang beredar, juga mencuri data pribadi untuk dijual kembali demi keuntungan, lemahnya keamanan pada sebuah server sehingga rentan diserang oleh pelaku dan meningkatnya *human error* akibat dari peningkatan penggunaan media online.

Solusi pencegahan yang dapat dilakukan dalam menghadapi ancaman siber yaitu dengan cara memperkuat aturan perundang-undang mengenai pencurian data pribadi, meningkatkan kerja sama keamanan siber menjadi salah satu strategi yang dapat dilaksanakan pemerintah Indonesia diharapkan dalam menyelenggarakan kerja sama baik bilateral maupun multilateral terutama terkait bidang keamanan siber dengan negara lain. Kerja sama antara pemerintah dengan pihak swasta diharapkan dapat ditingkatkan guna mendorong pertumbuhan ekonomi dan teknologi keamanan siber. Pencegahan lain yang dapat dilakukan secara individu yaitu dengan mencari informasi lebih lanjut mengenai berita yang diberikan oleh orang yang tidak dikenal dalam menggunakan sosial media, kemudian tidak asal mengklik postingan yang bukan dari sumber terpercaya atau orang yang tidak dikenal, serta bijak dalam memilih dan memilah informasi yang beredar di media sosial.

6. REFERENCES

[1] M. J. Islami, “TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX,” *Masy. Telematika Dan Inf. J. Penelit. Teknol. Inf. Dan Komun.*, vol. 8, no. 2, p. 137, Mar. 2018, doi: 10.17933/mti.v8i2.108.

[2] M. B. Satrio, “PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DALAM MEDIA ELEKTRONIK (ANALISIS KASUS KEBOCORAN DATA PENGGUNA FACEBOOK DI INDONESIA),” vol. 1, no. 1, p. 13, 2020.

[3] I. Rahmawati, “ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) DALAM PENINGKATAN CYBER DEFENSE,” p. 16.

[4] M. Fathur, “TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN,” p. 18.

[5] D. A. Sudarmadi and A. J. S. Runturambi, “Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia,” p. 21, 2019.

[6] “Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi.” https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi (accessed Nov. 30, 2021).

[7] “FEKDI 2021: BSSN Terus Berupaya Maksimalkan Keamanan Siber pada Sektor Ekonomi Digital | bssn.go.id.” https://bssn.go.id/fekdi-2021-bssn-terus-berupaya-maksimalkan-keamanan-siber-pada-sektor-ekonomi-digital/ (accessed Nov. 28, 2021).

[8] “Pusat Kajian Anggaran.” https://puskajianggaran.dpr.go.id/produk/detail-analisis-apbn/id/65 (accessed Nov. 30, 2021).

[9] B. Hartono, “HACKER DALAM PERSPEKTIF HUKUM INDONESIA,” no. 1, p. 8, 2014.

[10] “BSSN Publikasikan Hasil Monitoring Keamanan Siber Tahun 2020 | bssn.go.id.” https://bssn.go.id/bssn-publikasikan-hasil-monitoring-keamanan-siber-tahun-2020/ (accessed Nov. 30, 2021).

[11] E. N. Sarinastiti, “INTERNET DAN TERORISME: MENGUATNYA AKSI GLOBAL CYBER-TERRORISM MELALUI NEW MEDIA,” vol. 1, no. 1, p. 13, 2018.

[12] N. Sahrun, R. Roestam, and S. Defit, “Pengembangan Sistem Keamanan Jaringan Komputer Melalui Perumusan Aturan (Rule) Snort untuk Mencegah Serangan Synflood,” vol. 1, no. 2, p. 8, 2015.

[13] A. R. Arianto, “MEMBANGUN PERTAHANAN DAN KEAMANAN SIBER NASIONAL INDONESIA GUNA MENGHADAPI ANCAMAN SIBER GLOBAL MELALUI INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII),” p. 18.

[14] M. H. Rumlus and H. Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik," *J. HAM*, vol. 11, no. 2, p. 285, Aug. 2020, doi: 10.30641/ham.2020.11.285-299.
[15] S. Dewi, "KONSEP PERLINDUNGAN HUKUM ATAS PRIVASI DAN DATA PRIBADI DIKAITKAN DENGAN PENGGUNAAN CLOUD COMPUTING DI INDONESIA," p. 9, 2016.
[16] H. Niffari, "PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain," *J. Huk. Dan Bisnis Selisik*, vol. 6, no. 1, pp. 1–14, Jun. 2020, doi: 10.35814/selisik.v6i1.1699.
[17] A. A. Wd and P. Prananingtyas, "TANGGUNG JAWAB BANK PENERBIT (CARD ISSUER) TERHADAP KERUGIAN NASABAH KARTU KREDIT AKIBAT PENCURIAN DATA (CARDING) DALAM KEGIATAN TRANSAKSI," vol. 6, p. 13, 2017.
[18] M. M. Sumenge, "PENIPUAN MENGGUNAKAN MEDIA INTERNET BERUPA JUAL-BELI ONLINE," no. 4, p. 11.
[19] M. H. Wibowo and N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," vol. 1, p. 5.
[20] R. Wirawan, "Studi Kompetensi dan Kesadaran Pengguna E-Learning Terhadap Keamanan Sistem E-Learning Pada Pendidikan Tinggi," *ETHOS J. Penelit. Dan Pengabdi.*, vol. 7, no. 1, pp. 9–17, Jan. 2019, doi: 10.29313/ethos.v7i1.3850.
[21] S. A. Kusnadi, "PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI," *AL WASATH J. Ilmu Huk.*, vol. 2, no. 1, pp. 9–16, Apr. 2021, doi: 10.47776/alwasath.v2i1.127.