INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 6 Tahun 2023 Page 1135-1145
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia

Yusuf Daeng[1✉], Jimmy Levin[2], Karolina[3], Muhammad Razzaq Prayudha[4], Nindy Putri Ramadhani[5], Noverto[6], Susanto Imanuel[7], Virgio[8]
Jurusan Hukum, Fakultas Hukum, Universitas Lancang Kuning
Email: yusufdaeng23@gmail.com[1✉]

Abstrak

Dengan adanya kemajuan teknologi bukanlah tidak adanya tanpa sebuah persoalan, teknologi internet juga dapat menyebabkan kejahatan yang biasa di sebut Cyber Crime. Semakin pesatnya penggunaaaan teknologi maka semakin rawan untuk tingkat kejahatan yang dilakukan oleh orang-orang yang tidak bertanggung jawab untuk melakukan asiknya baik penipuan, pencurian, pencemaran nama baik serta kejahatan lainnya melalui internet. Dibentuklah perlindungan hukum terhadap korban cyber crime terdapat di dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Menurut Laporan National Cyber Security Index (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Adapun tujuan penulisan ini adalah Untuk mengetahui bagaimana penerapan sistem keamanan siber di Indonesia dan memahami hambatan penerapan sistem kemanan siber di Indonesia, serta upaya mengatasi hambatan dalam penerapan sistem kemanan siber supaya kejahatan siber di Indonesia bisa teratasi dan menurun Metode penelitian yang digunakan adalah studi kasus yang dimana kita meneliti lebih lanjut beberapa tulisan dari beragam sumber tentang kasus tersebut yang kemudian digunakan untuk mengidentifikasi dan menemukan permasalahan utama dari kasus yang sedang diteliti ini. Hasil penelitian menunjukkan bahwa benar sistem keamanan siber di Indonesia belum bisa mengantisipasi kejahatan siber dengan maksimal.

Kata Kunci: *Kejahatan Siber, Hukum Siber, Sistem Keamanan Siber*

Abstract

With technological advances it is not without problems, internet technology can also cause crimes which are usually called Cyber Crime. The more rapid the use of technology, the more prone it is to crimes committed by irresponsible people who commit fraud, theft, defamation and other crimes via the internet. The establishment of legal protection for victims of cyber crime is contained in Law Number 19 of 2016, an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. However, according to the National Cyber Security Index (NCSI) report, Indonesia's cyber security index score is 38.96 points out of 100 in 2022. This figure places Indonesia in the 3rd lowest ranking among the G20 countries. The purpose of this writing is to find out how the cyber security system is implemented in Indonesia and understand the obstacles to implementing the cyber security system in Indonesia, as well as efforts to overcome obstacles in implementing the cyber security system so that cyber crime in Indonesia can be overcome and reduced. The research method used is a case study in which we further examine several articles from various sources about the case which are then used to identify and find the main problems of the case being researched. The research results show that it is true that the cyber security system in Indonesia has not been able to anticipate cyber crime optimally.

Keywords: *Cyber Crime, Cyber Law, Cyber Security System*

PENDAHULUAN

Perkembangan masyarakat zaman sekarang ini semakin maju dan di dukung oleh pertumbuhan teknologi telekomunikasi, hingga ikatan antar negara sudah bersifat mendunia sehingga menghasilkan tatanan dunia baru (Budi Agus Riswandi, 2016). Demikian ini tidak dapat dipungkiri bahwa dampaknya terhadap perkembangan masyarakat Indonesia yang sedang membangun di era reformasi itu telah dihadapkan dengan berbagai krisis, baik politik, ekonomi, dan sosial budaya, dan ini harus ditangani agar bangsa dan negara Indonesia tetap dipandang keberadaannya di antara bangsa-bangsa di dunia (Angeline Xiao, 2018).

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global (Hendro Setyo Wahyudi & Mita Puspita Sukmasari, 2014). Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif perbuatan melawan hukum (Soecipto, 2022).

Indonesia dengan 202 juta pengguna internet saat ini telah menjadi salah satu penggerak ekonomi digital terbesar di Asia Tenggara. Pada tahun 2021 saja, ekonomi digital nasional telah memberikan kontribusi sebesar USD 70 miliar, dan diproyeksikan akan menembus USD 146 miliar pada 2025 mendatang. Namun demikian, pertumbuhan digital yang cepat ini juga diikuti dengan ancaman keamanan siber atau *cyber security* yang juga meningkat secara signifikan.

Laporan *National Cyber Security Index* (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Sementara secara global, Indonesia menduduki peringkat ke-83 dari 160 negara dalam daftar di laporan tersebut. NCSI membuat penilaian ini berdasarkan sejumlah indikator, seperti aturan hukum negara terkait keamanan siber, ada atau tidaknya lembaga pemerintah di bidang keamanan siber, kerja sama pemerintah terkait keamanan siber, serta bukti-bukti publik seperti situs resmi pemerintah atau program lain yang terkait. Jerman tercatat memiliki keamanan siber terbaik di antara negara G20 dengan skor 90,91 poin. Keamanan siber negara ini berada di peringkat ke-6 secara global. Berikutnya, Prancis berada di posisi kedua dengan skor keamanan siber tertinggi di antara negara G20 yakni sebesar 84,42 poin. Diikuti oleh Arab Saudi dengan skor indeks keamanan siber sebesar 83,12 poin, serta Amerika Serikat dan Italia dengan skor indeks masing-masing 79,22 poin. Sementara itu, sejumlah negara G20 lainnya yang berada di bawah peringkat Indonesia alias yang terendah yakni Meksiko dan Afrika Selatan. Skor indeks keamanan siber Meksiko sebesar 37,66 poin dan Afrika Selatan 36,36 poin.

Laporan terbaru dari National Cyber Security Index (NCSI) menunjukkan bahwa *cyber security* Indonesia berada di peringkat 6 di antara 10 negara di ASEAN, dan peringkat ke-83 dari 160 negara secara global.

Pada Januari 2019, 56% populasi Indonesia atau sekitar 150 juta orang menggunakan internet. Jumlahnya tumbuh 13% dari tahun sebelumnya. Pertumbuhan ini yang terbesar keempat di dunia setelah India, Cina, dan Amerika Serikat . Karena sistem keamanan siber yang kurang baik di Indonesia, negara ini sering mengalami serangan. Sebagai gambaran, selama satu minggu di bulan Februari, Indonesia menerima 1,35 juta serangan web. Serangan siber ini sebagian besar merupakan kasus peretasan, yang menargetkan situs web pemerintah dan perusahaan.

Perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar tekhnologi informasi, dalam penelitiannya menyatakan: "Kejahatan cyber (cyber crime) kini marak di lima kota besar di Indonesia dan

dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para hacker yang rata-rata anak muda yang keliatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet". Salah satu contoh kasus cyber crime yang sempat ramai diperbincangkan pada tahun 2020 lalu adalah kasus bocornya 91 juta data pengguna Tokopedia. Cyber crime dibagi menjadi 2 kategori, yakni cyber crime dalam pengertian sempit dan dalam pengertian luas. Cyber crime dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan cyber crime dalam arti luas mencakup kejahatan terhadap sistem ata Tujuan dari penelitian ini adalah untuk mengetahui bagaimana sistem keamanan siber serta menganalisis hambatan dan upaya untuk mengembangkan sistem keamanan siber di Indonesia.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur (library research) (P. Andi, 2012). Jenis pendekatan penelitian yang digunakan oleh peneliti di dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan teori dan asas hukum. Penelitian hukum normatif bisa juga disebut sebagai penelitian hukum doctrinal (Jonaedi Effendi dan Johnny Ibrahim, 2018).

Prosedur dalam penelitian ini dilaksanakan dengan tahapan-tahapan yaitu mengumpulkan data Pustaka, membaca, mencatat, menelaah, mengumpulkan konsep atau naskah kemudian dilakukan elaborasi dan eksplanasi terhadap data atau teks yang terkumpul berkaitan dengan topik pembahasan utama di dalam penelitian ini. Hal ini sesuai dengan pendapat Zed (M. Zed, 2008) yang mengatakan bahwa riset Pustaka tidak hanya sebatas urusan membaca dan mencatat literatur atau buku, melainkan serangkaian kegiatan yang berkenaan dengan metode pengumpulan data Pustaka, membaca, mencatat serta mengolah suatu bahan penelitian.

HASIL DAN PEMBAHASAN

Cyber crime merupakan tindakan kriminal yang menyerang sebuah komputer, jaringan komputer atau perangkat lainnya yang terhubung ke internet. Pelaku kejahatan siber dikenal sebagai hacker atau cybercriminal yang dijalankan secara individu atau tergabung dalam sebuah organisasi. Beberapa pelaku cyber crime memiliki skill mumpuni dan menggunakan teknik canggih sehingga mampu membobol website atau aplikasi dengan tingkat keamanan tinggi sekali pun (Didik M Arief Mansur & Elisatris Gultom, 2005).

Hacker atau kriminal siber melakukan cyber crime demi mendapatkan sejumlah uang dari tindakan ilegalnya. Ada pula alasan politis atau pribadi di balik aktivitas cyber

crime tersebut, meski motif ini jarang ditemukan karena rata-rata pelaku hanya mengincar keuntungan semata.

Jenis-jenis cyber crime yang mengancam keamanan computer yakni pemalsuan identitas, phising ,cracking, spoofing, serangan ddoS, carding, pemalsuan data, sim swap, botnet, cyberstalking, penipuan OTP, injeksi SQL, cyber espionage, serangan ransomware.

Pengaturan tindak pidana siber di Indonesia dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana ("KUHP") sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana ("UU 3/2011") maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang ("UU TPPU") (Renny N.S. Koloay, 2016).

Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 19/2016") sama halnya seperti *Convention on Cybercrimes*, UU ITE juga tidak memberikan definisi mengenai *cybercrimes*, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrimes* (Sitompul, 2012):

1. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:
    a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari (Musa Darwin Pane & Sahat Maruli Tua Situmeang, 2021):
        - Kesusilaan (Pasal 27 ayat (1) UU ITE);
        - Perjudian (Pasal 27 ayat (2) UU ITE);
        - penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE);
        - pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE);
        - berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE);
        - menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);
        - mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

b. dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE);
c. intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU 19/2016);

2. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:
   a. Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* - Pasal 32 UU ITE);
   b. Gangguan terhadap Sistem Elektronik (*system interference* –Pasal 33 UU ITE);
3. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);
4. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);
5. Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE); dan
6. Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu (Supanto, 2016):

a. Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* - Pasal 32 UU ITE);
b. Gangguan terhadap Sistem Elektronik (*system interference* –Pasal 33 UU ITE);
   1. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);
   2. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);
   3. Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE); dan
   4. Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Selain mengatur tindak pidana siber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP") dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

a. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika;
b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;
c. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana;
d. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

Adapun prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut:

1. Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian *Cybercrime* atau kepada penyidik PPNS pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam UU ITE.
2. Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPNS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI.

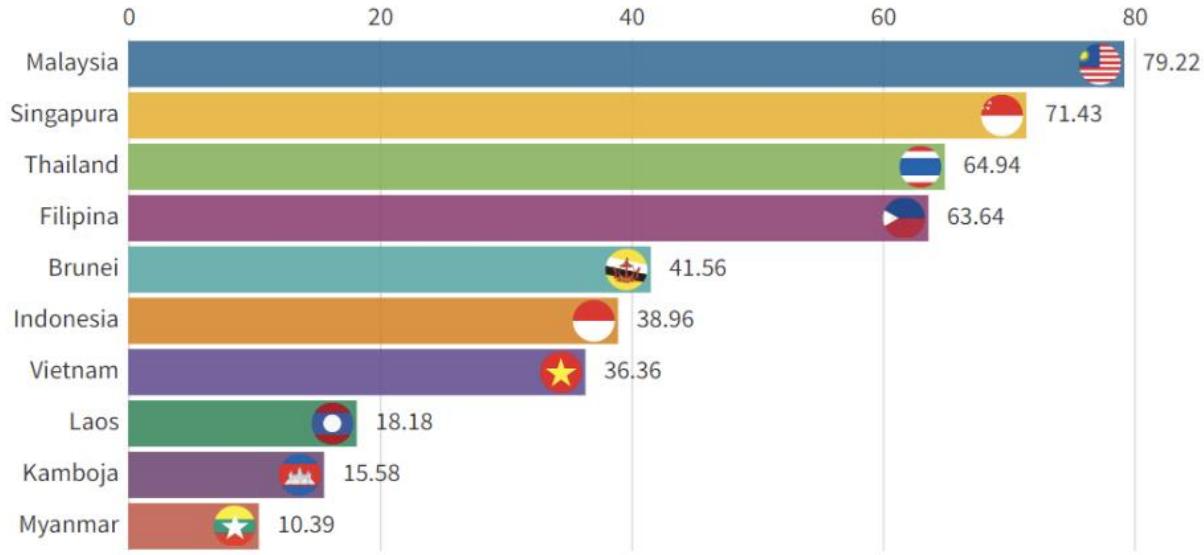
Selain UU ITE, peraturan yang menjadi landasan dalam penanganan kasus *cybercrime* di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Salah satu contoh kasus cyber crime yang sempat ramai diperbincangkan pada tahun 2020 lalu adalah kasus bocornya 91 juta data pengguna Tokopedia. Kasus ini diawali dengan cuitan akun @underthebreach di Twitter yang mengklaim bahwasanya 91 juta data pengguna aplikasi e-commerce tersebut sedang dijual di black market bernama RaidForums. Adapun data yang diperjualbelikan tersebut adalah User ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor handphone dan password dari pengguna aplikasi tersebut.

Kasus lainnya yakni kebocoran 18,5 juta data pengguna BPJS Ketenagakerjaan yang dijual di forum gelap seharga Rp153 juta, Minggu (12/3).Dalam sebuah unggahan di BreachForums, penjahat siber Bjorka membocorkan 19,5 juta data dengan nama 'BPJS Ketenagakerjaan Indonesia 19 Million'.Ia juga membagikan 100 ribu sampel yang berisi NIK, nama lengkap, tanggal lahir, alamat, nomor ponsel, alamat email, jenis pekerjaan dan nama perusahaan.

Dan juga pada 16 Mei 2023, data miliki Bank Syariah Indonesia (BSI) diduga mengalami kebocoran. Kala itu, pendiri Ethical Hacker Indonesia Teguh Aprianto mengungkap BSI menjadi korban serangan siber modus pemerasan alias ransomware oleh peretas LockBit. Total data yg dicuri mencapai 1,5 TB, termasuk 15 juta data pengguna dan password untuk akses internal dan layanannya, serta data pribadi nasabah serta informasi pinjamannya.

Menurut Laporan National Cyber Security Index (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Sementara secara global, Indonesia menduduki peringkat ke-83 dari 160 negara dalam daftar di laporan tersebut.



Sumber : Breached.to

Faktor faktor yang mempengaruhi performa keamanan siber suatu negara yakni

1. Ketersediaan departemen spesialisasi teknologi operasional khusus

Hampir setiap perusahaan industri memiliki sejenis tim keamanan teknologi operasional (OT). Namun, seringkali alih-alih membuat dan mendanai departemen keamanan OT, pekerjaan tersebut ditugaskan ke departemen keamanan TI atau bahkan departemen TI umum. Menruut Kaspersky departemen- departemen ini tidak selalu memahami spesifikasi teknologi operasional yang cukup untuk memberikan tingkat perlindungan yang diperlukan. Untuk meminimalkan risiko dan konsekuensi insiden di jaringan industri, perusahaan membutuhkan tim keamanan OT yang memiliki sumber daya terbaik dan berkualitas.

,

2. Proses pengambilan keputusan yang terstruktur dengan jelas

Seringkali masalah dalam sebuah perusahaan industri muncul karena kesalahan organisasi, ketika manajemen keamanan terdiri atas departemen yang tidak terkait satu sama lain. Akibatnya, perusahaan membeli solusi keamanan yang menduplikasi fungsi satu sama lain, visibilitas proses industri menjadi kurang memadai, data yang dikumpulkan dari titik akhir dan sensor digunakan secara tidak efisien, dan implementasi proyek baru tertunda karena persetujuan yang rumit.

3. Memiliki strategi manajemen infrastruktur legasi

Keamanan siber industri (*Industrial control system*/ICS) sering menggunakan peralatan yang dibuat sebelum orang memiliki gambaran kasar tentang tingkat digitalisasi industri modern yang akan datang. Oleh karena itu, sangat diperlukan kehati-hatian dalam membangun sistem kontrol untuk rangkaian jaringan industri yang sudah usang atau ketinggalan zaman, pengontrol logika yang dapat diprogram, sistem kontrol pengawasan dan akuisisi data (SCADA), dan elemen OT lainnya.

4. Memperkenalkan solusi keamanan yang dirancang khusus untuk ekosistem industry

Tidak mungkin untuk menyerahkan keamanan lingkungan ICS menggunakan solusi keamanan siber standar. Mereka dapat secara efektif mengatasi serangan siber umum secara acak, namun tidak akan mendeteksi ancaman khusus untuk proses industri. Selain itu, terkadang mereka dapat secara negatif mempengaruhi kelangsungan proses teknologi. Untuk menghindari hal ini, Kaspersky menyarakan untuk memiliki solusi yang dirancang khusus untuk lingkungan

5. Memiliki strategi konvergensi OT/TI dengan mempertimbangkan IIoT

Meningkatnya digitalisasi proses industri menyiratkan peningkatan tingkat integrasi antara lingkungan OT dan TI. Menurut Kaspersky, elemen kunci dari integrasi ini adalah penggunaan perangkat *Industrial Internet of Things* (IIoT), layanan cloud publik, dan gateway IIoT. "Semua elemen ini sering menjadi kerentanan di mana penyerang dapat mencapai sistem industri. Tidak realistis untuk menghentikan proses evolusi digital ini, oleh karena itu perlu untuk mengembangkan rencana dalam mengintegrasikan teknologi operasional dan informasi secara aman terlebih dahulu," kata Kirill Naboyshchikov, *Business Development Manager,* Kaspersky Industrial CyberSecurity.

6. Respon insiden secara cepat

Dengan satu atau lain cara, insiden tidak mungkin sepenuhnya dihindari. Tetapi ketika itu benar-benar terjadi, sangat penting bahwa akar masalah dapat diidentifikasi dan diatasi secepat mungkin. Semakin cepat dilakukan, semakin sedikit biaya yang dikeluarkan perusahaan baik secara finansial maupun reputasi. "Oleh karena itu, sangat penting bagi

perusahaan industri untuk memiliki regulasi respons cepat yang matang dan tim yang mampu melakukannya," kata Kirill.

7. Mempertimbangkan pelatihan staf dengan serius

Terakhir, Kaspersky menyarankan untuk tidak melupakan pentingnya perilaku yang berpusat pada keamanan dari karyawan perusahaan. Jika ingin meminimalkan dampak insiden terkait keamanan, melatih staf tentang dasar-dasar keamanan dan secara ketat memantau kepatuhan terhadap peraturan internal diperlukan. "Dengan satu atau lain cara, faktor manusia berada di balik sebagian besar insiden: seseorang secara tidak disadari menggunakan kata sandi pribadi yang disusupi, menghubungkan telepon ke komputer di balik celah udara, mengklik tautan ke situs web berbahaya, dan seterusnya. Setiap orang harus memahami dengan jelas apa yang bisa dan tidak bisa dilakukan di perusahaan industri, terutama jika itu merupakan fasilitas infrastruktur penting dan kritikal," terang Kirill.

SIMPULAN

Indonesia sudah melakukan berbagai cara untuk bisa memberantas kasus pidana siber diindonesia, akan tetapi sampai saat ini hal terssebut masih menjadi sebuah tantangan yang dimana menurut data Laporan National Cyber Security Index (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Sementara secara global, Indonesia menduduki peringkat ke-83 dari 160 negara dalam daftar di laporan tersebut. Beragam kasus yang terjadi mulai dari pencurian data, pishing dll sangat merugikan negara dan masyarakat, beberapa kasus seperti kasus pencurian data di bank bsi, bpjs dan imigrasi. Jika dibandingkan dengan keamanan siber di negara maju seperti amerika, cina, rusia , lemahnya kemanaan siber diindonesia bisa terjadi dikarenakan pengaruh infrastruktur dan teknologi yang masih rendah, pendidikan dan keterampilan rendah, anggaran keamanan siber yang masih rendah, kesadaran masyarakat yang masih rendah, struktur kebijakan dan regulasi yang masih belum berjalan dengan baik. Jadi bukan tidak ada tidak ada tindakan dari negara untuk menangani kejahatan siber diindonesia , indonesia telah mendirikan BSSN sebagai lembaga yang bertanggung jawab atas keamanan siber nasional. BSSN memiliki peran dalam mengkoordinasikan upaya keamanan siber di seluruh sektor pemerintah dan swasta, Kerjasama dengan negara maju untuk pengembangan sistem keamanan siber di Indonesia seperti Kerjasama tahun 2023 ini dengan negara Korea. Hanya saja dikarenakan sdm, modal dan infrastruktur yang terbatas mengakibatkan kurang maksimalnya performa sistem keamanan siber diindonesia. Dengan langkah-langkah ini, Indonesia

dapat meningkatkan keamanan sibernya dan melangkah menuju sistem keamanan yang lebih baik seperti negara maju. Namun perlu di ingat pengembangan dan perbaikan keamanan siber adalah tantangan yang terus berkembang, dan upaya terus ditingkatkan untuk menghadapinya serta melibatkan berbagai pemangku kepentingan.

DAFTAR PUSTAKA

Angeline Xiao. (2018). KONSEP INTERAKSI SOSIAL DALAM KOMUNIKASI, TEKNOLOGI, MASYARAKAT. Jurnal Komunikasi, Media Dan Informatika, 7(2), 94.

Budi Agus Riswandi. (2016). Hukum dan Teknologi: Model Kolaborasi Hukum dan Teknologi dalam Kerangka Perlindungan Hak Cipta di Internet. Jurnal Hukum IUS QUIA IUSTUM, 3(23), 346.

Didik M Arief Mansur, & Elisatris Gultom. (2005). Cyber Law Aspek Hukum Teknologi Informasi. Refika Aditama.

Hendro Setyo Wahyudi, & Mita Puspita Sukmasari. (2014). TEKNOLOGI DAN KEHIDUPAN MASYARAKAT. Jurnal Analisa Sosiologi, 3(1), 13.

Jonaedi Effendi, & Johnny Ibrahim. (2018). Metode Penelitian Hukum Normatif dan Empiris. Kencana.

M. Zed. (2008). Metode Penelitian Kepustakaan. Yayasan Obor Indonesia.

Musa Darwin Pane, & Sahat Maruli Tua Situmeang. (2021). Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi . Jurnal Loyalitas Sosial, 3(2), 94.

P. Andi. (2012). Metode Penelitian Kualitatif dalam Perspektif Rancangan Penelitian. Ar-Ruzz Media.

Renny N.S. Koloay. (2016). PERKEMBANGAN HUKUM INDONESIA BERKENAAN DENGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI. Jurnal Hukum Unsrat, 22(5), 16.

Soecipto. (2022). Optimalisasi Hukum Siber (cyber law) Dalam Penanggulangan Kejahatan Penipuan Melalui Internet dalam Menyelamatkan Kehidupan Masyarakat. Jurnal Teknologi Nusantara, 4(2), 35.

Supanto. (2016). PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY. Yustisia, 5(1), 53.