Jurnal Ilmu Komputer Revolusioner

Vol.8 No.2, Febuari 2024
ISSN: 24430355

ANALISIS KEAMANAN SIBER (*CYBER SECURITY*) DALAM ERA DIGITAL "TANTANGAN DAN STRATEGI PENGAMANAN"

Muslim[1], Amanda Sephira[2], Muhammad Hanif Abrar[3],
Semmy Loreno Suranta Perangin Angin[4], Habiebie Hidayatullah[5]
Universitas Pembangunan Panca Budi Medan
E-mail: ochaim251225@gmail.com[1], mandasephira21@gmail.com[2],
hanifabrarmohammad22@gmail.com[3], semlourboi@gmail.com[4], lubish711@gmail.com[5]

Abstrak

Keamanan sistem informasi telah menjadi isu penting di era digital saat ini. Artikel ini membahas tantangan utama yang dihadapi organisasi dalam memastikan keamanan sistem TI mereka dan menyajikan strategi keamanan yang efektif untuk mengatasi tantangan ini. Ancaman seperti serangan malware, phishing, dan ancaman orang dalam menjadi semakin kompleks dan seringkali memerlukan pendekatan yang komprehensif. Strategi penting untuk diterapkan dalam konteks ini adalah enkripsi data, pemantauan keamanan waktu nyata, dan pelatihan karyawan tentang keamanan. Dengan memperkuat pertahanan dan meningkatkan kesadaran akan ancaman keamanan, organisasi dapat mengurangi kemungkinan terjadinya insiden keamanan yang merugikan.
Kata Kunci: Keamanan Sistem Informasi, Era Digital, Tantangan, Strategi Pengamanan.

Abstract

Information system security is the main focus in the current digital era. This article discusses the main challenges that organizations face in ensuring the security of their information systems and presents effective security strategies to overcome these challenges. Threats such as malware attacks, phishing and insider threats are increasingly complex and often require a comprehensive approach. In this context, data encryption, real-time security monitoring, and security training for employees are important strategies to implement. By strengthening their defenses and increasing awareness of security risks, organizations can reduce the likelihood of costly security incidents occurring.
Keywords: *Information Systems Security, Digital Era, Challenges, Security Strategies.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan kontribusi positif terhadap pembangunan ekonomi global dalam beberapa dekade terakhir, yang mengarah pada produktivitas, daya saing, dan partisipasi masyarakat yang lebih besar. Namun, seiring dengan semakin terhubungnya pemerintah, dunia usaha, dan masyarakat di dunia maya, beberapa tantangan ancaman siber memerlukan perhatian lebih besar untuk menjamin keamanan siber yang lebih baik. Menurut ISO (Organisasi Internasional untuk Standardisasi), ISO/IEC 27032, mengutip berbagai sumber, keamanan informasi atau keamanan dunia maya mengacu pada menjaga kerahasiaan, integritas, dan ketersediaan informasi di dunia maya. Dunia maya mengacu pada lingkungan yang kompleks dan merupakan hasil interaksi antara manusia, perangkat lunak, dan layanan Internet melalui penggunaan berbagai perangkat teknologi dan berbagai koneksi jaringan serta lingkungan

informal. Menurut Kaspersky, keamanan siber adalah tentang melindungi pengguna komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya.Demikian pula, Cisco mendefinisikan keamanan siber sebagai praktik melindungi berbagai sistem, jaringan, dan program dari serangan digital.Oleh karena itu, keamanan siber atau keamanan informasi adalah tentang melindungi informasi di dunia maya dari berbagai serangan. Keamanan siber menjadi semakin populer karena meningkatnya penggunaan komputer seperti desktop, laptop, ponsel pintar, server, dan perangkat IoT (Internet of Things), serta penggunaan jaringan komputer seperti Internet dalam kehidupan masyarakat sehari-hari. Dalam kasus Indonesia, menurut BSSN (Badan Siber dan Sandi Negara), sejak Januari hingga Agustus tahun lalu, hampir 190 juta upaya serangan siber terjadi di Indonesia, meningkat sebesar empat dibandingkan tahun sebelumnya sesuai dengan periode 2019... atau sekitar 39 juta. . Banyak situs juga percaya bahwa serangan siber akan terus berlanjut pada tahun 2021. Kaspersky misalnya, mengatakan pandemi Covid-19 dapat memicu berbagai gelombang kemiskinan yang dapat meningkatkan kejahatan, termasuk serangan siber.Indonesia sangat membutuhkan strategi keamanan siber nasional di era Society 5.0 saat ini. Jika keamanan berarti terlindungi dari ancaman dan bahaya, salah satu faktor terpenting yang mempengaruhi manajemen keamanan siber adalah bagaimana memahami ancaman di dunia siber dan kemudian mencari solusinya. Tanpa langkah-langkah keamanan siber yang tepat, kemungkinan ancaman akan meningkat. Tantangan utama saat ini adalah penguatan lembaga yang bertanggung jawab atas keamanan siber, kurangnya landasan hukum untuk keamanan siber, dan kurangnya personel terampil serta kerja sama di dalam dan luar negeri.Oleh karena itu, penting bagi pemerintah untuk memperkuat keamanan siber dan mempersiapkan orang-orang yang diperlukan untuk menghadapi dunia yang semakin digital. Undang-Undang Keamanan Siber juga harus segera disahkan agar Indonesia dapat memulai upaya keamanan nasional terhadap meningkatnya serangan siber di era Society 5.0 saat ini. Keamanan siber adalah perlindungan sistem komputer, jaringan, dan data dari ancaman yang berkembang pesat seperti serangan malware, intrusi, dan pencurian identitas. Dalam konteks ini, era digital mempunyai konsekuensi penting karena memberikan peluang lebih besar bagi oknum-oknum yang tidak bertanggung jawab untuk mengeksploitasi kerentanan sistem.Keberlanjutan operasional, integritas data, dan keamanan informasi merupakan isu yang sangat penting untuk dipertimbangkan. Di era digital yang semakin maju, keamanan siber menjadi isu yang sangat penting. Teknologi informasi dan komunikasi tidak hanya memberikan banyak manfaat bagi kita, tetapi juga membuka pintu bagi serangan siber yang dapat merugikan individu, organisasi, dan bahkan negara. Dalam artikel ini, kami mengkaji tantangan keamanan siber, peran teknologidalam serangan dan perlindungan, serta solusi untuk mengatasi ancaman di dunia digital.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif dengan pendekatan sastra. Studi Literatur, Karena banyaknya informasi dan data mengenai strategi keamanan siber, studi literatur dilakukan. Hal ini dapat dipahami dari berbagai informasi di buku, jurnal ilmiah, surat kabar, majalah, serta sumber informasi dari situs internet. Studi literatur penting untuk menganalisis konsep strategi keamanan siber di Indonesia. Fasepertama terdiri dari pemilihan sumber dokumenter tentang keamanan siber, infrastruktur TI, dan teknologi terkait. Tujuan memperoleh informasi yang mendalam terutama terdapat pada jurnal ilmiah, buku teks, laporan penelitian, dan artikel berita.Setelah memilih sumber, penelitian terdiri dari tinjauan rinci dan analisis literatur

yang dipilih. Analisis ini terutama berfokus pada kerangka keamanan yang umum digunakan, tren ancaman siber saat ini, serta teknologi dan strategi keamanan yang efektif dalam melindungi infrastruktur TI. Hasil literatur kemudian dibagi ke dalam kategori utama seperti aspek teknis, kebijakan keamanan, pelatihan staf dan integrasi teknologi keamanan. Tujuannya adalah untuk memberikan pemahaman yang lebih sistematis tentang elemen-elemen kunci yang mempengaruhi keamanan infrastruktur TI. Pengembangan penelitian ini didasarkan pada pengetahuan mendalam tentang bidang-bidang yang informasinya mungkin tidak mencukupi atau memerlukan penelitian lebih lanjut.

3. HASIL DAN PEMBAHASAN

Cyber Crime di Indonesia

Munculnya kejahatan siber dimulai pada tahun 1988. Saat itu, kejahatan ini dikenal dengan nama serangan siber. Selama ini, penulis mengembangkan worm atau virus yang menyerang komputer dan menonaktifkan total sekitar 10% komputer yang terhubung ke Internet di seluruh dunia. Cybercrime adalah suatu kegiatan atau peristiwa yang melibatkan teknologi komputer dimana seseorang memperoleh keuntungan dengan menimbulkan kerugian pada pihak lain. Cybercrime juga merupakan kejahatan komputer yang dilakukan oleh individu atau sekelompok orang yang menyerang sistem keamanan komputer atau data yang terkandung di dalamnya. Kejahatan-kejahatan ini dilakukan karena berbagai alasan, mulai dari kepuasan diri sendiri hingga kejahatan yang dapat menimbulkan kerugian ekonomi atau politik.Contoh kejahatan dunia maya mencakup ancaman keamanan siber seperti rekayasa sosial, eksploitasi kerentanan perangkat lunak, dan serangan jaringan.

Secara umum, kejahatan dunia maya adalah kejahatan yang dilakukan dengan menggunakan teknologi komputer sebagai alat kriminal utama. Dengan kata lain, seseorang memanfaatkan kemajuan teknologi untuk melakukan kejahatan. Serangan siber menimbulkan ancaman yang mengerikan bagi banyak orang saat ini, terutama para wirausaha. Diketahui, banyak perusahaan di seluruh dunia mengalami kerugian finansial hingga $1 triliun pada tahun 2020 akibat pandemi virus corona ketika hampir semua perusahaan menerapkan kebijakan bekerja dari rumah (WFH), yang berujung pada pelonggaran aturan. keamanan digital.Menurut laporan baru dari Center for Strategic and International Studies (CSIS) dan McAfee Cybersecurity, perkiraan kerugian sebesar $945 miliar hampir dua kali lipat kerugian finansial akibat kejahatan dunia maya, yaitu $500 miliar pada tahun 2018.

Berdasarkan kajian Direktorat Kejahatan Siber (Dittipidsiber) Bareskrim Polri, Indonesia mencatat 90 juta kasus serangan siber dan menurut Financial Services Information Exchange and Analysis Center (FS-ISAC), Indonesia masuk dalam daftar negara rentan. terhadap serangan kejahatan dunia maya. Indonesia sendiri berada di peringkat 9. Pandemi Covid-19 menjadi topik utama dalam tren keamanan siber. Peretas memanfaatkan kerusuhan tersebut dengan melancarkan serangan mulai dari phishing hingga ransomware, membobol data 91 juta pengguna situs belanja online Tokopedia, dan mengungkap data 1,2 juta pengguna situs Bhinneka.Indonesia juga terkena dampak dari kasus keamanan siber global seperti ransomware virus corona, malware Covidlock, peretasan Border Gateway Protocol, kerentanan router Draytek Vigor, eksekusi kode jarak jauh di beberapa versi produk sistem operasi Windows, dan kerentanan eksekusi kode arbitrer di seluruh sistem operasi Google Android. Produk platform Solar Winds Orion. Masa pandemi juga menjadi sasaran empuk bagi para peretas yang terus berusaha menembus sistem keamanan perusahaan karena intensifnya penggunaan Internet saat hampir semua orang bekerja dari rumah. Data BSSN menunjukkan serangan terbanyak

tercatat pada Maret 2020, sebanyak 22 serangan siber terjadi selama pandemi COVID-19. Serangan ini mencakup berbagai jenis serangan termasuk HawkEye Reborn Trojan, Blackwater Malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, Netwalker Ransomware, Cerberus Banking Trojan, Ursnif Malware, AdobotSpyware, Metasploit Downloader Trojan, Projectspy Spyware, Anubis Banking Trojan. Adware, iklan tersembunyi (Android), spyware AhMyth, Metasploit, Xerxes Bot, dan aplikasi pelacakan Covid19.

Tantangan Dan Strategi Keamanan Cyber

Tantangan Cyber

a. Perkembangan Teknologi: Perkembangan teknologi yang pesat menciptakan tantangan baru bagi keamanan siber. Semakin banyak perangkat yang terhubung ke Internet, semakin besar potensi kerentanan yang dapat dieksploitasi oleh penyerang. Selain itu, penyerang dapat memanfaatkan teknologi seperti kecerdasan buatan dan komputasi awan untuk melancarkan serangan yang lebih canggih dan kompleks.
b. Serangan Berasal dari Berbagai Pihak: Serangan siber dilakukan tidak hanya oleh individu atau kelompok tertentu, namun juga oleh negara atau kelompok terorganisir. Serangan-serangan ini dapat berupa pencurian data, sabotase, dan bahkan serangan siber yang dapat menghancurkan infrastruktur penting suatu negara. Meningkatnya intensitas dan variasi serangan meningkatkan kompleksitas perlindungan sistem dan data.
c. Kekurangan Pakar Keamanan Cyber: Kekurangan pakar keamanan siber merupakan masalah serius. Permintaan akan tenaga profesional keamanan siber yang berkualifikasi jauh melebihi pasokan yang tersedia. Hal ini menciptakan kesenjangan dalam perlindungan dan membatasi kemampuan perusahaan untuk merespons dan mencegah serangan siber.
d. Sosial Teknik Serangan: Penyerang sering menggunakan teknik media sosial dalam serangannya. Mereka mengeksploitasi ketidaktahuan, kelalaian, atau kecerdasan emosional korban untuk mendapatkan akses tidak sah atau informasi sensitif. Metode paling populer yang digunakan oleh penyerang adalah serangan phishing, serangan spear phishing, atau serangan rekayasa sosial.
e. Kelemahan Sistem dan Aplikasi: Kerentanan pada sistem operasi, perangkat lunak, atau aplikasi merupakan kerentanan yang sering dieksploitasi oleh penyerang. Kerentanan yang tidak terdeteksi atau perangkat lunak yang tidak diperbarui secara rutin dapat menjadi pintu gerbang serangan siber.
f. Keberlanjutan Ancaman: Ancaman keamanan siber tidak pernah berakhir. Penyerang terus mengembangkan teknik dan metode baru untuk menghindari deteksi dan menggagalkan upaya pertahanan. Ancaman yang berkembang dan berubah secara dinamis memerlukan respon yang cepat dan adaptif untuk menjaga keamanan sistem dan data.

Tantangan saat ini dalam memperkuat keamanan siber meliputi: Kurangnya ketersediaan pakar teknologi dan pakar keamanan teknis untuk merancang dan menerapkan strategi keamanan siber. Ancaman ini muncul dari sifat keamanan siber yang bersifat lintas batas negara, yang berarti bahwa negara-negara dengan strategi ketahanan keamanan siber yang lemah dapat membahayakan keamanan siber negara lain.Penggunaan alat anonimisasi, misalnya untuk memblokir rantai mata uang atau enkripsi, dalam kejahatan dunia maya semakin mempersulit pembuatan kebijakan. Munculnya teknologi dan sistem baru memerlukan pembaruan sistem pemantauan secara berkala dari waktu ke waktu. Terdapat jenis penyedia layanan telekomunikasi baru, yang seringkali berbasis di luar negeri, yang memerlukan perlakuan berbeda dibandingkan perusahaan telekomunikasi tradisional. Bentuk-bentuk baru kejahatan dunia maya seperti ransomware, pencurian identitas, grooming, dan pelecehan seksual dunia maya. Karena kurangnya

peraturan dan regulasi internasional yang mengatur perilaku negara, kita harus menghadapi serangan dunia maya dan bentuk konflik antar negara lainnya.

Strategi Keamanan Cyber

Strategi keamanan

Strategi keamanan siber adalah serangkaian tindakan, kebijakan, dan praktik yang dirancang untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari serangan siber dan ancaman keamanan lainnya. Strategi keamanan siber seringkali bersifat holistik dan mencakup berbagai pendekatan untuk membendung ancaman dan merespons potensi serangan.Berikut adalah beberapa strategi keamanan cyber yang umum digunakan:

1. Pengenalanan Ancaman (Threat Intelligence): Strategi ini melibatkan pengumpulan informasi tentang potensi ancaman dunia maya, termasuk jenis serangan, pola serangan, dan taktik penyerang. Informasi ini digunakan untuk lebih memahami potensi ancaman dan mengembangkan strategi pertahanan yang efektif.
2. Pelatihan dan Kesadaran Pengguna: Mendidik pengguna tentang praktik keamanan terbaik adalah bagian penting dari strategi keamanan siber. Pelatihan ini dapat mencakup pengenalan tentang phishing, praktik perlindungan kata sandi, dan mengenali tanda-tanda serangan siber.
3. Kebijakan Keamanan: Mengembangkan kebijakan keamanan yang jelas dan ketat merupakan elemen kunci dari strategi keamanan siber. Kebijakan ini mencakup penggunaan kata sandi yang kuat, pembatasan akses ke data sensitif, dan tindakan respons insiden keamanan.
4. Pemantauan dan Deteksi Dini: Strategi ini melibatkan penerapan alat pemantauan dan deteksi yang memungkinkan organisasi mendeteksi dan merespons serangan siber dengan cepat sebelum terjadi kerusakan signifikan.
5. Pembaruan Perangkat Lunak: Pembaruan perangkat lunak secara berkala merupakan strategi keamanan siber yang penting. Pembaruan perangkat lunak mengatasi kerentanan dalam sistem operasi, aplikasi, dan perangkat lunak lain yang dapat dieksploitasi oleh penyerang.
6. Enkripsi Data: Melindungi data dengan enkripsi adalah strategi yang efektif untuk mencegah akses tidak sah. Enkripsi data mengubah informasi menjadi format yang tidak dapat dibaca tanpa kunci enkripsi yang sesuai.
7. Manajemen Akses: Menerapkan prinsip hak istimewa paling rendah pada manajemen akses membantu mengurangi risiko serangan. Ini berarti bahwa pengguna atau sistem diberikan hak akses minimum yang diperlukan untuk menjalankan tugasnya.
8. Pencadangan dan Pemulihan: Mencadangkan data Anda secara teratur dan mengembangkan rencana pemulihan bencana adalah strategi penting ketika menghadapi serangan dunia maya. Dengan pencadangan rutin, perusahaan dapat memulihkan data dan sistem mereka setelah serangan.
9. Kolaborasi dan Kemitraan: Berkolaborasi dengan lembaga keamanan siber lainnya dan berbagi intelijen ancaman siber merupakan strategi penting dalam memerangi serangan siber lintas negara yang kompleks.

Dengan menerapkan strategi keamanan siber yang holistik dan proaktif, perusahaan dapat mengurangi risiko serangan siber dan meminimalkan dampak serangan.

Strategi Penguatan Cyber Security di Indonesia

Capacity Building.

Program pelatihan dan pengembangan keterampilan keamanan siber dilaksanakan berkoordinasi dengan tim kerja Pusat Operasi Pertahanan Siber. Selain itu, pengembangan sumber daya manusia mengenai pentingnya keamanan siber sangat penting untuk lebih memahami langkah-langkah pencegahan untuk mencegah kejahatan siber. Membangun kembali sistem pertahanan berbasis pertahanan siber dan keamanan siber tentunya memerlukan persiapan yang matang dan sistematis dengan dukunganaktor berbeda.

Sinergi dalam menghadapi ancaman siber merupakan sebuah keniscayaan dan kebutuhan saat ini bagi Indonesia. Melalui sinergi dan komunikasi, koordinasi, networking dan kerjasama teknis, komunitas keamanan siber yang mampu menghalau, mendeteksi, menghalangi dan mencegah berbagai potensi serangan siber harus diciptakan untuk memperkuat keamanan dan ketahanan nasional.Fungsi BSSN saat ini menuai kritik karena tumpang tindih secara signifikan dengan institusi seperti Kementerian Komunikasi dan Informatika, Unit Kejahatan Siber Polri, dan Pusat Operasi Siber Kementerian Pertahanan Negara. Ke depan, Indonesia harus mempercepat pengesahan UU Keamanan Siber agar tercipta landasan hukumnya.

Keberadaan undang-undang ini juga dapat mendorong pengembangan strategi keamanan siber nasional yang komprehensif yang dapat mendefinisikan fungsi BSSN dengan lebih baik. Untuk itu, perlu dilakukan adaptasi strategi keamanan siberuntuk transformasi digital menuju solusi keamanan berlapis. Tingkat pertama berisi unit kerja, baik tim IT maupun tim bisnis.Persyaratan keamanan, kesadaran keamanan, kemampuan merancang solusi aman yang menjamin pengalaman menyenangkan. Pada tingkat kedua terdapat tim manajemen risiko dan kepatuhan. Tim ini harus memiliki wawasan yang lengkap dan terkini mengenai ancaman keamanan siber agar bisa berdiskusi bersama. Pada tingkat ketiga, terdapat tim audit yang tugasnya memeriksa apakah pengendalian keamanan TI sudah memadai atau belum dan perlu ditingkatkan. Tim audit harus memiliki keterampilan dan pengetahuan yang sesuai untuk mengatasi ancaman keamanan siber saat ini. Yakni, kemampuan untuk memverifikasi keamanan cloud, pengembangan tangkas, dll.Mengingat pentingnya keamanan siber, terdapat kebutuhan mendesak untuk memperkuat lembaga yang bertanggung jawab mengoordinasikan upaya dengan dukungan penuh dari seluruh pemangku kepentingan bila diperlukan. Lembaga koordinator harus terdiri dari orang-orang yang berintegritas dan berkompeten tinggi. Pada tingkat operasional, setiap sektor harus memiliki tim tanggap daruratnya sendiri untuk menangani insiden di sektornya, dan masing-masingmemiliki peran dan tanggung jawab yang jelas.

Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber.

Kurangnya landasan hukum keamanan siber berdampak pada struktur organisasi yang seharusnya mengaturnya. Tanpa dasar hukum ini, mustahil penerapan praktik keamanan siber di tingkat nasional. Hal ini juga menciptakan kebingungan dalam mengoordinasikan tanggung jawab keamanan siber. RUU Keamanan Siber saat ini tidak dibuka untuk umum: hanya versi undang-undang sebelumnya yang tersedia, namun naskah akademis UUjuga tersedia. Undang-undang dan peraturan teknologi informasi di Indonesia saat ini belum mencakup semua kejahatan siber, sehingga ada beberapa kejahatan siber yang terkena dampaknya. saat ini merupakan permasalahan keamanan dan pertahanan (sebagai salah satu faktor dalam menjaga keamanan dan kedaulatan negara) yang belum diatur dalam peraturan nasional.Harus ada undang-undang khusus untuk kejahatan dunia maya di Indonesia. Aturan khusus ini menetapkan prinsip-prinsip umum yang berlaku untuk semua pelanggaran yang berkaitan dengan teknologi informasi dan komunikasi, pelanggaran yang berkaitan dengan kerahasiaan, integritas dan ketersediaan data atau sistem TI/telematika, pedoman pidana, hukum acara dalam pelaksanaan persidangan, dll. .berlaku untuk penyidikan hal-hal di bidang teknologi informasi dan komunikasi, termasuk penggeledahan dan penyitaanbarang bukti digital, kerja sama internasional dalam pemberantasan kejahatan dunia maya. Faktanya, Indonesia rentan terhadap serangan siber dan terdapat kesenjangan hukum dalam penanganannya. Undang-undang dan peraturan keamanan siber di Indonesia membagi tanggung jawab antar kementerian dan dianggap tidak efektif dalam mencegah ancaman dan kejahatan siber.

Oleh karena itu, peraturan keamanan siberyang komprehensif sangat dibutuhkan di

Indonesia.Oleh karena itu, undang-undang keamanan siber harus secara jelas mendefinisikan dan menjelaskan peran, tanggung jawab, dan wewenang lembaga terkait untuk mengatasi ancaman keamanan siber. Dalam mempertimbangkan RUU ini, DPR dan BSSN harus menginisiasi dialog swasta-pemerintah atau public-private dialog (PPD). PPD terbukti membantu berbagi informasi dan pengalaman yang relevan, mengembangkan kebijakan yang lebih tepat sasaran dan diterapkan dengan baik, serta mendapatkan dukungan luas daripemangku kepentingan.

Peningkatan Sumberdaya Manusia

Sumber daya manusia merupakan salah satu elemen terpenting untuk memastikan keamanan siber diterapkan sesuai pedoman yang telah ditetapkan. Anda harus memperoleh dan mempertahankan pengetahuan dan keterampilan khusus seiring dengan berkembangnya kebutuhan keamanan Anda. Sumber daya manusia dilaksanakan melalui program rekrutmen, pengembangan, dan pemberhentian sesuai dengan peraturan perundang-undangan yang berlaku. Masyarakat sering kali menjadi titik lemah dalam rantai keamanan. Tidak peduli seberapa hati-hati Anda,kali orang bisa tersandung dan melakukan kesalahan sebagai pengguna.Dan untuk itu Terkait keamanan siber, meningkatkan kesadaran tentangsangatlah penting. Dengan mengelola sumber daya manusia, teknologi, dan penelitian dan pengembangan (Litbang) untuk memperkuat keamanan siber, pemerintah dalam hal ini Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi bekerja sama dengan BSSN dan Kementerian Komunikasi dan Informatika harus mengambil langkah-langkah inovatif. tindakan mengambil upaya solusi. Melatih dan merekrut profesional keamanan siber dengan integritas dan etika sempurna untuk mendukung pengembangan dan implementasi keamanan siber. Misalnya, salah satu pendekatan teknis adalah dengan menggunakan ISO 25010 untuk menguji aplikasi Android atau web guna membantu memantau keamanan data serta antarmuka yang lebih baik dan pemfilteran konten pornografi di Internet. Dengan perencanaan dan pengujian aplikasi yang tepat, Anda mengurangi risiko peretas menyalahgunakan berbagai aplikasi, informasi, dan pusat data di Internet.

Peran Teknologi Dalam Serangan Dan Perlindungan

1. Malware dan Ransomware

Malware dan ransomware adalah ancaman yang biasa dieksploitasi oleh penyerang. Malware adalah perangkat lunak berbahaya yang bertujuan untuk merusak atau mengambil kendali suatu sistem. Ransomware adalah jenis malware yang mengenkripsi data dan meminta uang tebusan untuk menerima kunci dekripsi. Melindungi sistem dari serangan semacam itu memerlukan teknologi deteksi dan deteksi malware yang canggih.

2. Serangan DdoS

Serangan DDoS (Distributed Denial of Service) dirancang untuk mencegah pengguna mengakses sistem atau situs web dengan membanjiri lalu lintas jaringan. Penyerang menggunakan jaringan komputer atau botnet yang terinfeksi untuk melancarkan serangan DDoS. Untuk menjaga ketersediaan layanan online, diperlukan teknologi mitigasi DDoS yang kuat dan terukur.

3. Serangan Phishing

Serangan phishing berupaya mendapatkan informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi dengan menyamar sebagai entitas tepercaya melalui email, SMS, atau situs web palsu. Pelatihan pengguna dan teknologi pendeteksi phishing yang efektif dapat membantu mencegah serangan ini.

4. Serangan Zero-Day

Serangan zero-day merupakan serangan yang mengeksploitasi kerentanan keamanan yang belum diketahui pelakunya. Hal ini memberikan keuntungan bagi penyerang karena

tidak ada pembaruan atau langkah keamanan yang tersedia untuk mengatasi kerentanan. Untuk mendeteksi dan menghilangkan serangan zero-day, diperlukan penelitian dan pengembangan teknologi inovatif.

5. Keamanan Cloud

Layanan komputasi awan telah menjadi bagian integral dari banyak bisnis, namun layanan ini juga menghadirkan tantangan keamanan yang unik. Keamanan cloud mencakup perlindungan data, enkripsi, identifikasi akses yang tepat, dan pemantauan yang cermat. Teknologi dan kebijakan keamanan cloud yang kuat diperlukan untuk melindungi data yang disimpan dan diproses di lingkungan cloud.

Solusi dalam Keamanan Cyber

a. Kesadaran dan Pendidikan Pengguna

Penting untuk mewaspadai ancaman keamanan siber dan mengedukasi pengguna tentang praktik keamanan yang baik. Pengguna harus menerima informasi dan pelatihan tentang cara menggunakan perangkat dan layanan digital dengan aman serta cara mengenali dan melaporkan serangan siber.

b. Pemantauan dan Deteksi yang Kuat

Untuk mendeteksi serangan siber dengan cepat, Anda perlu menggunakan teknologi pemantauan dan deteksi yang andal. Dengan memantau lalu lintas jaringan, aktivitas pengguna, dan log sistem, Anda dapat mendeteksi serangan sejak dini dan mengambil tindakan yang tepat.

c. Enkripsi dan Keamanan Data

Data yang disimpan dan diproses harus dienkripsi menggunakan metode yang kuat. Enkripsi yang tepat pada tingkat file, jaringan, dan aplikasi dapat melindungi data dari akses yang tidak sah. Selain itu, praktik keamanan data seperti pencadangan dan pemulihan rutin juga penting untuk melindungi data dari kehilangan atau kerusakan.

d. Pembaruan dan Pemeliharaan Perangkat Lunak

Memastikan sistem dan perangkat lunak selalu diperbarui dengan patch keamanan terbaru sangat penting. Pembaruan perangkat lunak rutin dan pemeliharaan yang baik dapat mengurangi risiko penyerangan yang memanfaatkan kelemahan yang diketahui.

e. Kolaborasi dan Kerjasama

Kolaborasi antara organisasi, pemerintah, dan lembaga keamanan siber sangat penting untuk memerangi serangan siber. Berbagi informasi tentang ancaman dan serangan yang terdeteksi serta mengembangkan praktik keamanan bersama dapat membantu memperkuat pertahanan dan respons terhadap serangan siber.

Tantangan keamanan siber terus meningkat seiring kemajuan teknologi. Penyerang terus mencari kerentanan baru dan metode serangan yang lebih canggih. Oleh karena itu, penting untuk terus mengembangkan solusi keamanan siber yang efektif.Berikut adalah beberapa langkah tambahan yang dapat diambil untuk mengatasi tantangan dalam keamanan cyber:

a) Analisis Ancaman dan Intelijen Keamanan

Melakukan penilaian ancaman dan memperoleh intelijen keamanan yang relevan dapat membantu mendeteksi dan memprediksi serangan siber. Mengumpulkan informasi tentang tren serangan saat ini, metode serangan yang digunakan, dan calon pelaku dapat membantu Anda mengidentifikasi potensi ancaman dan mengambil tindakan yang tepat.

b) Penerapan Kebijakan Keamanan yang Ketat

Organisasi harus menerapkan kebijakan keamanan yang ketat dan memastikan bahwa semua anggota tim mengikuti protokol keamanan yang ditetapkan. Hal ini mencakup praktik keamanan seperti penggunaan kata sandi yang kuat, kebijakan akses yang membatasi, dan penggunaan alat keamanan seperti firewall dan program antivirus.

c) Pemantauan Identitas dan Akses Pengguna

Melacak identitas dan akses pengguna dapat membantu mendeteksi aktivitas tersebut Nomormencurigakan atau tidak valid. Penggunaan teknologi autentikasi dua faktor dan protokol audit dapat membantu mendeteksi serangan yang melibatkan akses tidak sah atau penyalahgunaan akun.

d) Pelatihan Keamanan Cyber

Menyelenggarakan pelatihan keamanan siber bagi karyawan merupakan langkah penting dalam meningkatkan kesadaran dan kerentanan terhadap serangan siber. Pelatihan ini mungkin mencakup pengenalan jenis serangan, taktik penipuan yang umum, dan praktik terbaik keamanan. Dengan pengetahuan yang benar, karyawan dapat berperan aktif dalam melindungi sistem dan data perusahaan.

e) Kolaborasi dengan Pihak Ketiga

Bekerja sama dengan penyedia layanan keamanan siber atau konsultan keamanan dapat membantu Anda meningkatkan pertahanan dan respons terhadap serangan. Penyedia layanan keamanan siber dapat memberikan pemantauan dan deteksi tingkat lanjut serta rekomendasi kebijakan keamanan yang diperlukan. Berkolaborasi dengan pihak ketiga juga dapat memberikan wawasan baru dan dukungan ahli dalam menghadapi ancaman siber yang semakin kompleks.

Di dunia digital yang terus berkembang, keamanan siber merupakan tantangan yang perlu ditangani secara serius. Dengan mengambil pendekatan holistik dan menggabungkan teknologi, kebijakan, dan praktik terbaik, kita dapat mengurangi risiko serangan siber serta melindungi data dan sistem yang berharga. Keamanan siber bukan hanya tanggung jawab seseorang atau organisasi tertentu, namun merupakan tanggung jawab bersama kita semua. Melalui kolaborasi, kerja sama, dan inovasi, kita dapat menciptakan lingkungan digital yang aman dan tepercaya bagi semua orang.

4. KESIMPULAN

Keamanan siber adalah isu yang semakin mendesak di era digital saat ini. Seiring dengan kemajuan teknologi yang pesat, tantangan pemeliharaan sistem dan keamanan data menjadi semakin kompleks. Namun, dengan pendekatan yang tepat dan solusi yang efektif, kita dapat mengurangi risiko serangan siber dan melindungi informasi berharga. Pelatihan pengguna, pemantauan yang efektif, enkripsi data, pembaruan perangkat lunak, dan kolaborasi yang baik adalah beberapa langkah penting untuk memastikan keamanan siber. Melalui upaya bersama, kita dapat menciptakan lingkungan digital yang aman dan andal.Penelitian ini masih jauh dari sempurna dan evolusi ancaman dunia maya semakin meluas dan sulit dihentikan. Oleh karena itu, penelitian yang lebih teknis harus dilakukan untuk memperkuat keamanan siber dan menjawab tantangan dunia global di masa depan.

DAFTAR PUSTAKA

Aliya, Kupas Tuntas Cybersecurity dan Seluk-beluknya, https://glints.com/id/lowongan/cybersecurityadalah/#. YYYucmBBzIU (Diakses tanggal 2 November 2021)

Cakrawala, Apa Itu Cyber security? Mengapa Cyber security Kini Makin Penting? https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa-cyber-security-kinimakin penting?page=all (Diakses tanggal 2 November 2021)

Creswell, J. W., & Plano Clark, V. L. (1993). Qualitative Research: A Review of the Methods and Techniques. Journal of Social Work Education, 29(3), Fall 1993.

Humaira Dasep Lukiman, Cyber security: Apa Itu Cyber security?, https://wakool.id/blog/582-cyber-security-apa-itu cyber-security (Diakses tanggal 2 November 2021)

Hasyim Gautama, Penerapan Cyber security, http://kemhubri.dephub.go.id/pusdatin files/materi/Penerapan_Cybersecurity.pdf. (Diakses tanggal 2 November 2021)"Apa itu

Cyber Crime" https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/ (Diakses tanggal 1 November 2021)
ITU. 2020. Global Cybersecurity Index 2020. International Telecommunication Unit Indonesia's data accessible and downloadable on https://ncsi.ega.ee/country/id/
Kompas.com. 2019. RI Rugi Rp 478,8 Triliun akibat Serangan Siber, DPR Siapkan RUU diakses dari https://nasional.kompas.com/read/2019/08/12/13454311/ri-rugi-rp-4788-triliun-akibat-serangan-siber-dpr siapkan-ruu-kks?page=all pada 20 Juli 2021
Pusat Operasi Keamanan Siber Nasional, Laporan Tahun 2020 (Monitoring Keamanan Siber). Jakarta: Badan Siber Dan Sandi Negara, 2020
Sanjaya, B. R., Efrianti, D., Ali, M., Prasetyo, T., Mukhtadi, M., Widasari, Y. K., & Khumairoh, Z. (2022). Pengembangan Cyber Security dalam Menghadapi Cyber Warfare di Indonesia. Journal of Advanced Research in Defense and Security Studies, 1(1), 19-34. Available online at: https://ejournal.hakhara institute.org/index.php/JARDS
Sautunnida, L, 2018," Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi perbandingan Hukum Inggris dan Malaysia", Kanun Jurnal Ilmu Hukum