Jurnal Informasi dan Teknologi

https://jidt.org/jidt

2023 Vol. 5 No. 3 Hal: 20-25 e-ISSN: 2714-9730

Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia

Irwan Dermawan✉, Asmat Baidawi, Iksan, Selly Mellyana Dewi

Universitas Madura

darmawan@unira.ac.id

Abstrak

Dengan perkembangan teknologi informasi, para penjahat menggunakan berbagai ruang cyber untuk meningkatkan kejahatan cyber. Risiko dan serangan cyber telah berkembang menjadi area utama yang menjadi perhatian. Karena telah terjadi peningkatan yang sangat besar dalam serangan cyber, serangan-serangan tersebut menyebabkan serangkaian kerusakan pada proses perbankan yang kritis dan menyebabkan kerugian finansial yang sangat besar pada sistem. Untuk memoderasi kejahatan cyber dan ancaman cyber, industri keuangan berupaya menerapkan kecerdasan buatan dan keamanan siber lainnya untuk meningkatkan pengalaman pelanggan dan efisiensi proses perbankan. Dengan demikian, penelitian saat ini datang untuk menilai dan menguji pengalaman perbankan Indonesia dengan serangan cyber dengan mengungkap reaksi sistem keamanan cyber terhadap serangan cyber dan apakah serangan cyber mempromosikan intersistem bank dan memotivasi mereka untuk meningkatkan tindakan pencegahan mereka untuk menyelamatkan basis data dan server bank dari pelanggaran. Penelitian ini menggunakan kuesioner sebagai alat utama untuk mengumpulkan data responden tentang bagaimana mereka mengalami serangan cyber setidaknya dua tahun yang lalu. Temuan yang signifikan adalah bahwa bank-bank Indonesisa mempertahankan tingkat keamanan tertentu terlepas dari apakah ada serangan hebat atau tidak. Namun, beberapa responden masih berhati-hati dalam menggunakan layanan perbankan online karena rendahnya keamanan akses publik ke layanan internet di Indonesia.

Kata Kunci: Serangan Cyber, Keamanan Cyber, Peretasan, Bank Indonesia.

1. Pendahuluan

Sektor perbankan dan keuangan merupakan sektor besar dengan jumlah nasabah yang besar di seluruh dunia. Sepanjang tahun ini, aksesibilitas layanan perbankan kepada kelompok masyarakat yang paling lemah atau paling rentan terus meningkat. Menurut database Findex globe tahun 2017, ditemukan bahwa terdapat 1,2 miliar orang dewasa yang memiliki rekening bank. Selain itu, terlihat bahwa sebagian besar negara beralih ke pendekatan digital; sekitar 51% lebih memilih saluran perbankan online sementara 26% mengakses layanan melalui situs web bank dan menggunakan layanan mobile banking.

Karena pesatnya pertumbuhan digitalisasi di bank, risiko dan serangan cyber telah berkembang menjadi area utama yang menjadi perhatian. Selama beberapa dekade terakhir, telah terjadi peningkatan serangan siber yang sangat besar, dan serangan tersebut menyebabkan serangkaian kerusakan pada proses perbankan yang kritis dan menyebabkan kerugian finansial yang besar pada sistem. Sangat penting bagi sektor perbankan atau keuangan untuk menerapkan strategi keamanan cyber yang efektif.

Strategi keamanan siber yang efektif seperti kecerdasan buatan (AI) untuk mengatasi semua masalah ini. Dengan demikian, studi saat ini akan menjelaskan kondisi keamanan siber di bank-bank swasta Indonesia dan apakah bank-bank tersebut menawarkan tingkat yang dapat diterima untuk melindungi dirinya sendiri dan menjaga basis data pelanggannya.

2. Landasan Teori

Serangan dunia maya dapat didefinisikan sebagai serangan yang didorong oleh penyerang dengan bantuan lebih dari satu komputer atau jaringan. Serangan semacam itu dapat dengan sengaja mempengaruhi sistem serta dapat mencuri data. Ini dapat dilakukan dengan menggunakan komputer yang disusupi.

Penjahat dunia maya mematuhi berbagai pendekatan untuk diajukan serangan dunia maya, termasuk pengelabuan, penipuan kartu ATM/Debit/Kredit, dan banyak lainnya. Serangan dunia maya terutama dirancang untuk menyebabkan kerusakan keuntungan.

Selain itu, penjahat dunia maya sering membuat alat perangkat lunak yang membantu mereka menggunakan serangan dan sering membagikannya di web gelap untuk mencapai tujuan. Ini sering muncul di tingkat awal dengan mendeteksi atau memindai penyerang mencari kerentanan atau titik masuk yang memulai kerja sama awal

Diterima: 26-06-2023 | Revisi: 01-07-2023 | Diterbitkan: 21-08-2023 | doi: 10.60083/jidt.v5i3.364

kemudian melakukan seluruh serangan, apakah itu untuk mencuri informasi penting dengan menonaktifkan sistem komputer atau keduanya

Seorang peretas dapat melakukan serangan dunia maya dengan berbagai cara untuk mencuri, memodifikasi, atau menghapus data atau bukti. Di mana metode utamanya adalah penolakan layanan, di mana DDoS menyerang sumber daya sistem sehingga tidak dapat kembali ke layanan yang diinginkan. Tapi ini satu-satunya yang didorong karena sejumlah besar mesin host lain terpengaruh oleh perangkat lunak berbahaya yang diorganisir oleh penyerang.

Serangan banjir TCP SYN adalah jenis lain dari serangan dunia maya, di mana penyerang memanfaatkan penggunaan ruang buffer melalui mekanisme transmisi sesi protokol jabat tangan. Perangkat penyerang membanjiri tujuan sistem baris kecil yang sedang berlangsung dengan permintaan penautan, tetapi ketika sistem target membalasnya, itu tidak merespons.

a. Pengelabuan

Ini hanyalah salah satu dari banyak penipuan di internet, mencoba mengelabui orang agar meninggalkan uang mereka. Mengacu pada penerimaan pesan spontan oleh klien lembaga keuangan, meminta mereka untuk memasukkan nama pengguna, kata sandi, atau informasi pribadi lainnya untuk masuk ke akun mereka karena alasan yang tidak diketahui.

Klien dikoordinasikan ke tiruan palsu dari situs pendirian pertama ketika mereka mengklik koneksi pada email untuk memasukkan data mereka, sehingga mereka tetap tidak mengetahui bahwa pemerasan telah terjadi. Penipu kemudian mendekati saldo keuangan online klien dan aset yang terkandung dalam catatan itu. Phishing adalah demonstrasi pengiriman email ke klien secara tidak jujur yang mengaku sebagai upaya nyata yang diatur mencoba mengelabui klien agar memberikan data pribadi yang akan digunakan untuk penipuan. Email tersebut memandu klien untuk mengunjungi situs web tempat mereka didekati untuk memperbarui data individu, seperti kata sandi dan Visa, asisten pensiun federal, dan nomor buku besar, yang sudah dimiliki oleh asosiasi asli. Halaman Web, bagaimanapun, palsu dan diatur hanya untuk mengambil data klien.

Misalnya, tahun 2003 melihat penggandaan trik phishing di mana klien mungkin mendapatkan pesan bahwa asosiasi asli sudah memiliki. Halaman Web, bagaimanapun, palsu dan diatur hanya untuk mengambil data klien. Misalnya, tahun 2003 melihat penggandaan trik phishing di mana klien mungkin mendapatkan pesan bahwa asosiasi asli sudah memiliki.

Halaman Web, bagaimanapun, palsu dan diatur hanya untuk mengambil data klien. Misalnya, tahun 2003 melihat penggandaan di mana klien mungkin mendapatkan pesan eBay menjamin bahwa akun klien akan ditangguhkan kecuali jika dia mengetuk antarmuka yang diberikan dan memperbarui data Visa yang dimiliki eBay sebelumnya. Karena agak mudah untuk membuat halaman web terlihat seperti situs web asosiasi asli dengan meniru kode HTML, triknya bergantung pada individu yang tertipu dengan spekulasi bahwa mereka benar-benar dijangkau oleh eBay dan akibatnya membuka halaman web eBay untuk menyegarkan catatan mereka data.

Dengan mengirim spam ke sekelompok besar orang, "phisher" mengandalkan email yang dibaca oleh sejumlah orang yang benar-benar telah mencatat nomor kartu kredit di eBay. Phishing, juga disebut sebagai karikatur atau pemeriksaan merek, adalah penyimpangan kecil dari "memancing", pemikiran bahwa iming-iming dibuang dengan harapan bahwa sementara sebagian besar akan mengabaikan jerat, beberapa akan terpikat untuk menggerogoti.

Phishing adalah teknik misrepresentasi email di mana pelakunya menyampaikan email sekilas asli yang mencoba mengumpulkan data pribadi dan keuangan dari penerima. Biasanya, pesan tersebut tampaknya berasal dari situs web yang terkenal dan dapat diandalkan. Situs yang sering diparodikan oleh phisher antara lain PayPal, eBay, MSN, Yahoo, Best Buy, dan America Online. Sebuah usaha phishing, mirip dengan perjalanan memancing namanya, adalah usaha spekulatif: Menempatkan undian berharap untuk mengelabui beberapa mangsa yang masuk perangkap. Phisher menggunakan berbagai desain sosial yang berbeda dan taktik parodi email untuk mencoba menipu.

b. Tindakan Pencegahan

Secara keseluruhan, saat ini, Anda memahami alamat bahaya kejahatan dunia maya, apa saja cara terbaik untuk melindungi PC dan informasi Anda sendiri? Tetap perbarui pemrograman dan kerangka kerja Menjaga produk dan kerangka kerja Anda berpikiran maju menjamin bahwa Anda mendapat untung dengan tambalan keamanan terbaru untuk memastikan PC Anda

Gunakan perangkat lunak anti-infeksi dan perbarui terus-menerus Menggunakan perangkat lunak anti-infeksi atau solusi keamanan web lengkap seperti Kaspersky Total Security adalah cara cerdas untuk melindungi sistem Anda dari serangan. Pemrograman terhadap infeksi memungkinkan Anda untuk memeriksa, membedakan, dan menghilangkan bahaya sebelum menjadi masalah. Memiliki pengaturan keamanan ini membantu melindungi PC

dan data Anda dari kejahatan dunia maya, memberi Anda sedikit akal. Jika Anda menggunakan perangkat lunak anti- infeksi, pastikan Anda tetap memperbaruinya untuk mendapatkan tingkat perlindungan terbaik.
Gunakan kata sandi yang kuat Pastikan untuk menggunakan kata sandi yang kuat untuk individu tidak akan mencari dan tidak merekamnya di mana pun. Atau gunakan pemimpin kata rahasia yang terhormat untuk membuat kata sandi yang kuat secara acak untuk membuatnya lebih mudah. pembuat kunci rahasia sewenang- wenang dan tidak sulit untuk diingat. Kata sandi yang solid tidak boleh berisi data individu. Jangan pernah membuka tautan dalam pesan spam, cara yang patut dicontoh yang membuat PC tercemar oleh serangan malware dan jenis kejahatan dunia maya lainnya adalah melalui tautan email dalam pesan spam. Jangan pernah membuka koneksi dari pengirim yang tidak Anda ketahui. Cobalah untuk tidak mengetuk tautan di pesan spam atau situs tidak tepercaya. Cara lain orang menjadi korban kejahatan dunia maya adalah dengan mengetuk tautan di pesan spam atau pesan lain, atau situs baru. Cobalah untuk tidak melakukan ini agar tetap aman di web.
Cobalah untuk tidak memberikan data dekat rumah kecuali jika aman Jangan pernah memberikan informasi dekat rumah melalui telepon atau melalui email kecuali jika Anda benar-benar yakin saluran atau email tersebut aman. Verifikasi bahwa Anda berbicara dengan orang yang Anda anggap sebagai Anda. Hubungi organisasi secara langsung tentang permintaan yang meragukan jika Anda mendapatkan informasi yang diminta dari organisasi yang menelepon Anda, tutup telepon. Hubungi mereka kembali menggunakan nomor di situs otoritas mereka untuk memastikan Anda menghubungi mereka dan bukan penjahat dunia maya.
Di dunia yang sempurna, gunakan telepon alternatif karena penjahat dunia maya dapat menunggu dengan ketat. Ketika Anda merasa telah menelepon ulang, mereka dapat mengklaim berasal dari bank atau asosiasi lain yang Anda yakini sedang Anda tuju. Waspadai URL situs mana yang Anda kunjungi, awasi URL yang Anda ketuk. Apakah mereka terlihat asli'? Cobalah untuk tidak mengetuk gabungan dengan URL baru atau yang tampak berbahaya.
Jika produk keamanan web Anda memiliki kegunaan untuk transaksi online, pastikan itu diaktifkan sebelum melakukan transaksi keuangan online. Hati- hati dengan pernyataan bank Anda, tip kami akan membantu Anda mencoba untuk tidak melakukan kejahatan dunia maya. Meskipun demikian, sebagai upaya terakhir, mendeteksi bahwa Anda telah menjadi korban dari Hati-hati dengan pernyataan bank Anda, tip kami akan membantu Anda mencoba untuk tidak melakukan kejahatan dunia maya. Meskipun demikian, sebagai upaya terakhir, mendeteksi bahwa Anda telah menjadi korban dari Hati-hati dengan pernyataan bank Anda, tip kami akan membantu Anda mencoba untuk tidak melakukan kejahatan dunia maya. Meskipun demikian, sebagai upaya terakhir, mendeteksi bahwa Anda telah menjadi korban dari kejahatan dunia maya dengan cepat adalah signifikan. Hati- hati dengan artikulasi bank Anda dan pertanyakan setiap pertukaran baru dengan bank. Bank dapat memeriksa apakah mereka menipu

c. Memerangi tantangann di bank

Pesatnya perkembangan teknologi komuter terdiri dari banyak faktor positif; Namun, teknologi ini juga menimbulkan masalah. Dimana permasalahan yang paling sering terjadi adalah penipuan dan pencurian dengan bantuan teknologi informasi. Jumlah dan kejahatan dunia maya meningkat dari hari ke hari dan baru saja melompat ke posisi kedua sebagai kejahatan ekonomi dan lembaga keuangan yang paling banyak dilaporkan sebagai target utama. Ini dilakukan oleh teknologi informasi dan pemantauan, kontrol, detasemen, dan pencegahan menjadi sangat sulit.
Beberapa serangan siber memberikan dampak langsung pada perbankan atau sistem organisasi seperti phishing. Tidak mudah untuk mendeteksi serangan semacam ini dan mengurangi masalah ini. Kemajuan dalam otomasi dan integrasi keamanan dianalisis dan beberapa produk dapat memberikan manfaat utama. Waktu respons diidentifikasi dengan benar, bersama dengan sumber daya yang langka ini terlibat dalam peningkatan produktivitas insinyur keamanan yang berbakat. Dengan demikian, dengan bantuan kecerdasan buatan, ancaman yang berkembang dapat diidentifikasi dengan mengumpulkan tanggapan bank terhadap kejahatan dunia maya. Penting untuk menilai implementasi kecerdasan buatan untuk memberikan keamanan siber berkualitas tinggi di bank karena dapat mempertahankan anggaran akhir.
Ada begitu banyak ancaman keamanan dunia maya di industri perbankan, yang paling umum adalah pencurian identitas, spoofing, dan layanan pihak ketiga yang tidak aman. Untuk memitigasi semua ancaman tersebut, industri perbankan dapat memastikan memiliki solusi keamanan yang tepat dengan mengedukasi karyawan agar dapat memeriksa keseluruhan sistem secara berkala. Oleh karena itu, sektor perbankan memiliki begitu banyak peluang untuk meningkatkan keamanan siber meskipun rentan.
Bank perlu meningkatkan pendekatan berwawasan ke depan terhadap keamanan siber. Langkah-langkah pencegahan sudah digunakan, termasuk firewall, aplikasi antivirus dan antimalware, dan pemindaian kerentanan. Padahal, dengan menerapkan beberapa lainnya

langkah-langkah intelijen seperti kecerdasan buatan (AI) yang diterapkan pada otentikasi pertama dengan bantuan akses biometrik untuk otentikasi multi-faktor (MFA), pertahanan dapat diperkuat. Misalnya menggunakan sidik jari untuk memverifikasi pembayaran dengan dompet digital seperti Apple Pay atau Google Pay.
Tantangan utama keamanan dunia maya adalah kerentanan yang melekat pada sistem dan perangkat lunak yang digunakan oleh titik akses bank yang tak terhitung jumlahnya terhadap teknologi pertahanan yang disengaja dan ketinggalan zaman yang sangat rentan terhadap teknologi serangan canggih yang digunakan oleh peretas. Namun, kesiapan keamanan dunia maya wajib adalah tujuan paling mendasar dari lembaga perbankan.
Meningkatnya adopsi media sosial mengarah pada potensi yang lebih besar untuk dieksploitasi oleh peretas. Banyak pengguna memposting data mereka atau siapa saja yang melihatnya. Yang berpotensi dapat dimanfaatkan untuk menyerang organisasi pengguna.
Menggunakan media sosial untuk menyebarkan berita palsu dapat berdampak buruk pada reputasi bank. Sebelum pengembangan chatbots, penelitian chatbots untuk peta layanan pelanggan berhasil dilakukan. d) Pengawasan cyber
Cyber Stalking adalah pemanfaatan internet atau sarana elektronik lainnya untuk mengikuti seseorang. Istilah ini digunakan secara timbal balik dengan pelecehan online dan penganiayaan online. Menindaklanjuti pada umumnya mencakup perilaku mengganggu atau merusak yang dilakukan seseorang berulang kali, seperti setelah seseorang, muncul di rumah atau lingkungan bisnis seseorang, membuat keputusan telepon yang mengganggu, meninggalkan pesan tertulis atau protes, atau merusak properti individu.
Cyber Stalking adalah "serangan" berbasis inovatif pada satu individu yang telah ditunjuk secara eksplisit untuk serangan itu karena alasan kemarahan, balas dendam, atau kontrol. Penguntit Cyber dapat mengambil banyak struktur, termasuk mendesak, mempermalukan, dan mempermalukan korban yang membersihkan saldo keuangan atau kontrol moneter lainnya. Misalnya, menghancurkan peringkat FICO korban yang mengganggu keluarga, teman, dan bisnis untuk melepaskan korban, istilah tersebut juga dapat diterapkan pada penguntit "konvensional" yang menggunakan teknologi untuk melacak dan menemukan korban dan perkembangannya dengan lebih efektif (misalnya, memanfaatkan peringatan Facebook untuk menyadari di pesta apa mereka bergabung).
Pengawasan digital asli' Harapannya adalah melukai korban yang direncanakan dengan memanfaatkan kerahasiaan dan jarak inovasi yang tidak bisa dilacak. Sebagai aturan, korban tidak pernah menemukan identitas penguntit digital yang menyakiti mereka, terlepas dari kehidupan mereka yang sepenuhnya dijungkirbalikkan oleh pelakunya.

d. Peretasan

"Peretasan" adalah kejahatan, yang melibatkan penghancuran kerangka kerja dan mendapatkan izin masuk yang tidak disetujui ke informasi yang disimpan di dalamnya. Peretasan telah melihat ekspansi 37 persen tahun ini. Contoh peretasan terkait dengan antarmuka online tertentu dan mendapatkan lokasi pribadi dari catatan email penduduk kota baru-baru ini terlihat. Saltines adalah orang-orang yang mencoba mendapatkan izin masuk ke PC yang tidak disetujui. Ini biasanya dilakukan dengan menggunakan program 'akses tidak langsung' yang diperkenalkan di mesin Anda. Banyak wafer juga mencoba mengakses aset menggunakan pemrograman pemecah frase rahasia, yang mencoba miliaran kata sandi untuk melacak kata sandi yang tepat untuk masuk ke PC. Jelas, keamanan yang layak dari ini adalah mengubah kata sandi secara konsisten. Dalam pengorganisasian PC, peretasan adalah pekerjaan khusus apa pun untuk mengontrol perilaku khas asosiasi organisasi dan kerangka kerja terkait. Seorang programmer adalah setiap individu yang sibuk dengan hacking.
Ungkapan "peretasan" umumnya mengacu pada pekerjaan khusus yang produktif dan tajam yang tidak benar-benar terkait dengan kerangka kerja PC. Hari ini, bagaimanapun, peretasan dan pemrogram paling sering dikaitkan dengan serangan pemrograman yang merusak di internet dan organisasi lain. Insinyur MIT selama tahun 1950-an dan 1960an awalnya mempromosikan istilah dan gagasan peretasan. Dimulai di klub kereta model dan kemudian di ruang PC server terpusat, "peretasan" yang seharusnya dilakukan oleh pemrogram ini diharapkan menjadi analisis khusus yang tidak berbahaya.
Latihan belajar yang menyenangkan. Setelah itu, di luar MIT, yang lain mulai menerapkan istilah tersebut untuk pengejaran yang kurang penting. Sebelum internet menjadi arus utama, misalnya, beberapa programmer di AS menjelajahi jalan yang berbeda mengenai cara mengganti telepon untuk membuat keputusan jarak jauh bebas melalui jaringan telepon secara ilegal. Ketika pengorganisasian PC dan internet meledak dalam prevalensi, jaringan informasi menjadi tujuan programmer dan peretasan yang paling terkenal.

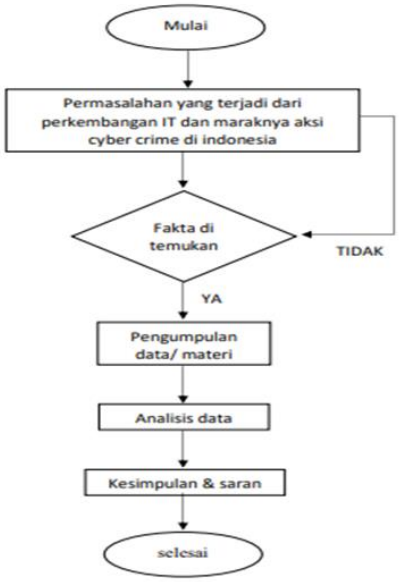
3. Metode Penelitian

Adapun langkah-langkah yang diambil dalam penelitian ini sebagai berikut :

1. Pengumpulan data: Mengumpulkan data yang relevan tentang serangan cyber yang terjadi pada Bank Indonesia serta informasi tentang keamanan cyber.

2. Analisis situasi : Menganalisa situasi serangan cyber yang pernah terjadi seperti jenis serangan, sasaran target, metode serangan yang digunakan, serta dampak yang ditimbulkan.
3. Survei dan wawancara: Melakukan survei terkait keamanan cyber untuk mengetahui tingkat kesiagaan dan kebijakan yang telah diimplementasikan. Serta, wawancara dengan ahli keamanan cyber eksternal guna mendapatkan perspektif tambahan.
4. Analisis data: Menganalisa data yang telah dikumpulkan dari berbagai sumber untuk mengidentifikasi kelemahan sistem serta menilai tingkat kesiapan serta efektivitas keamanan.
5. Pembahasan dan hasil: Membahas hasil penelitian yang mencakup tema utama, masalah keamanan cyber yang dihadapi, tingkat kesiapan, dan efektivitas sistem keamanan cyber.

Dengan flowchart cara penerapan:



Gambar 1. Karangka pemikiran

4. Hasil dan Pembahasan

Berdasarkan penelitian yang dilakukan, terdapat beberapa hasil terkait serangan cyber terhadap Bank Indonesia yakni sebagai berikut.

1. Jenis serangan: Analisis menunjukkan bahwasannya Bank Indonesia telah menghadapi berbagai jenis serangan cyber, termasuk serangan DdoS, malware, serta upaya pencurian data. Serangan-serangan ini menunjukkan kompleksitas dan tingkat ancaman yang tinggi terhadap Bank Indonesia.
2. Sasaran dan dampak: Serangan-serangan tersebut ditujukan pada sistem infrastruktur keuangan yang sensitif, termasuk sistem pembayaran, sistem informasi internal, serta data nasabah. Dampak yang ditimbulkan dari berbagai serangan tersebut seperti gangguan operasional, kehilangan data, serta kerugian finansial.
3. Kesiapan serta langkah-langkah keaman: Meskipun langkah keamanan telah diimplementasikan dengan baik, peneliti menunjukkan bahwasannya masih terdapat celah kurang kuatnya keamanan. Tingkat keamanan cyber harus ditingkatkan dengan memperbarui kebijakan, keamanan dalam penanganan serangan cyber.
4. Rekomendasi: Terdapat beberapa rekomendasi dari beberapa penelitian guna menigkatkan keamanan yang meliputi penignkatan pelatihan serta kesadaran kemanan cyber bagi Bank Indonesia, penerapan sistem keamanan yang lebih kuat dan terintegrasi, serta kerjasama kuat untuk memantau dan mengatasi ancaman yang mucul.

Pembahasan hasil penelitian dapat membantu Bank Indonesia dalam meningkatkan kesiagaan dan keamanan cyber, sehingga dapat mengurangi resiko serangan cyber serta melindungi aset data yang sensitif..

5. Kesimpulan

Keadaan saat ini di seluruh dunia, dampak pandemi dan perkembangannya memengaruhi semua sektor bisnis dan menimbulkan ketegangan yang sangat besar terhadap orangorang dengan menurunkan pendapatan mereka. Akibatnya, serangan siber meningkat secara global membawa tantangan baru bagi semua institusi dan terutama bagi bank dan lembaga keuangan. Oleh karena itu, penelitian kami datang sebagai upaya untuk mengungkap

tingkat kesiapan keamanan siber di bank swasta Indonesia. Akibatnya, penelitian ini mengungkapkan bahwa pelanggan kadangkadang menghadapi serangan siber, dan mereka masih mengkhawatirkan jenis kejahatan semacam itu.

Pada saat yang sama, bank swasta Indonesia melakukan yang terbaik untuk memperbarui dan membangun sistem keamanan siber mereka, baik ada serangan siber atau tidak. Karena cybersecurity menjadi isu kontemporer di zaman kita, bagaimanapun.

Daftar Rujukan

[1] Anwar, N., Hasan, MF, & Nasim, J. (2021). Peran Ajaran Islam dalam Membentuk Kesehatan Mental Remaja Terdidik : Sebuah Kontribusi menuju Good Governance. Jurnal Internasional Ilmu Sosial, Inovasi dan Teknologi Pendidikan, 2(7), 203–214.

[2] Kavousi-Fard, A., Su, W., & Jin, T. (2021). Model Deteksi Serangan Cyber Berbasis Pembelajaran Mesin untuk Jaringan Sensor Nirkabel di Microgrid. Transaksi IEEE pada Informatika Industri, 17(1), 650–658. https://doi.org/10.1109/TII.2020.2964704.

[3] Kalech, M. (2019). Deteksi serangan dunia maya dalam sistem SCADA menggunakan teknik pengenalan pola temporal. Komputer dan Keamanan, 84, 225–238. https://doi.org/10.1016/j.cose.2019.03.007

[4] Zhang, F., Kodituwakku, HADE, Hines, J. W., & Coble, J. (2019). Sistem Deteksi Serangan Cyber Multilayer Berbasis Data untuk Sistem Kontrol Industri Berdasarkan Jaringan, Sistem, dan Data Proses. Transaksi IEEE pada Informatika Industri, 15(7), 4362– 4369. https://doi.org/10.1109/TII.2019.2891261.

[5] Hasan, MF, & Al-Dahan, NS (2019). Efek penggembalaan investor domestik terhadap investor asing: Bukti dari bursa saham Irak. Jurnal Internasional Inovasi, Kreativitas dan Perubahan, 10(6), 234–245.

[6] Saha, S., Roy, TK, Mahmud, MA, Haque, SAYA, & Islam, SN (2018). Operasi mikrogrid DC yang tangguh terhadap kesalahan sensor dan serangan siber. Jurnal Internasional Tenaga Listrik dan Sistem Energi, 99, 540–554.https://doi.org/10.1016/j.ijepes.2018.01.007.

[7] Jakobsson, M., & Ramzan, Z. (2008). Crimeware: memahami serangan dan pertahanan baru. Dalam Teknik. Addison-WesleyProfesional. http://www.amazon.com/dp/0321501950.

[8] Flayyih, HH, Ali, SI, & Mohammed, YN (2018). Pengaruh Integrasi Mekanisme Tata Kelola Perusahaan dan Kualitas Audit pada PT Earning Management : Sebuah Analisis Empiris Bank Tercatat . Jurnal Internasional Teknik & Teknologi, 7(4), 337–344.

[9] Flayyih, HH, Ali, SI, & Mohammed, YN (2018). Pengaruh Integrasi Mekanisme Tata Kelola Perusahaan dan Kualitas Audit pada PT Earning Management : Sebuah Analisis Empiris Bank. Jurnal Internasional Teknik & Teknologi, 7(4), 337–344.

[10] Hasan, MF, & Al-Dahan, NS (2019). Efek penggembalaan investor domestik terhadap investor asing:. Jurnal Internasional Inovasi, Kreativitas dan Perubahan, 10(6), 234–245.

[11] Erickson, J. (2008). Peretasan: Seni Eksploitasi, Edisi ke-2. Di Majelis. Tidak ada patitekan. http://www.amazon.com/Hacking- Art- Exploitation-Jon-Erickson/dp/1593271441