KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.1 Februari 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 33-42
DOI: https://doi.org/10.61722/jmia.v2i1.3119

KEAMANAN SIBER DALAM PERBANKAN SERTA TANTANGAN DAN SOLUSI DI ERA DIGITAL

Diny Widya Evriyanti Simatangkir
Universitas Negeri Semarang
Eka Febriantika Nur afifah
Universitas Negeri Semarang
Nafiza Salsabila Faliha
Universitas Negeri Semarang

Alamat: Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah 50229
Korespondensi penulis: dinikir52@students.unnes.ac.id , ekafebriantika93@students.unnes.ac.id , nafizasf@students.unnes.ac.id

Abstrak. *The development of digital technology has brought about a major transformation in the banking industry, making services faster, more efficient and accessible. However, these advancements also present major challenges in the form of evolving cybersecurity threats. This research discusses the level of cyber threats faced by the banking sector, the main challenges in implementing an effective cybersecurity system, and innovative solutions to strengthen digital defences. Using a qualitative approach through literature review, this research identifies threats such as malware, phishing, ransomware, and DDoS attacks, and examines best practices in dealing with these risks. In addition, the proposed solutions include implementing the latest technologies such as artificial intelligence and blockchain, strengthening regulations, and increasing awareness and education for employees and customers. The results of this research are expected to contribute to the development of effective cybersecurity strategies to protect data, maintain customer trust, and ensure the operational stability of the banking sector in the digital era.*

Keywords: *Cyber, Banking, Threats, Digital Technology,*

Abstrak. Perkembangan teknologi digital telah membawa transformasi besar dalam industri perbankan, menjadikan layanan lebih cepat, efisien, dan mudah diakses. Namun, kemajuan ini juga menghadirkan tantangan besar berupa ancaman keamanan siber yang terus berkembang. Penelitian ini membahas tingkat ancaman siber yang dihadapi sektor perbankan, tantangan utama dalam penerapan sistem keamanan siber yang efektif, serta solusi inovatif untuk memperkuat pertahanan digital. Dengan pendekatan kualitatif melalui studi literatur, penelitian ini mengidentifikasi berbagai ancaman seperti malware, phishing, ransomware, dan serangan DDoS, serta mengkaji praktik terbaik dalam menghadapi risiko tersebut. Selain itu, solusi yang diusulkan meliputi penerapan teknologi terkini seperti kecerdasan buatan dan blockchain, penguatan regulasi, serta peningkatan kesadaran dan edukasi bagi karyawan dan nasabah. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan strategi keamanan siber yang efektif untuk melindungi data, menjaga kepercayaan nasabah, dan memastikan stabilitas operasional sektor perbankan di era digital.

Kata Kunci: : *Siber, Perbankan, Ancaman, Teknologi Digital.*

Received Desember, 2024; Revised Desember, 2024; Februari 2, 2025
*

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan. Digitalisasi memungkinkan layanan perbankan menjadi lebih cepat, efisien, dan mudah diakses oleh nasabah di mana saja dan kapan saja. Namun, di balik berbagai kemudahan tersebut, ancaman terhadap keamanan siber menjadi salah satu risiko terbesar yang harus dihadapi. Keamanan siber dalam perbankan menjadi isu yang sangat krusial seiring dengan pesatnya perkembangan teknologi digital. Perbankan modern kini semakin bergantung pada sistem digital untuk memberikan layanan kepada nasabah, mulai dari transaksi online hingga pengelolaan data yang sensitif. Namun, semakin banyaknya layanan digital ini juga membawa dampak negatif berupa peningkatan ancaman siber. Serangan siber yang dapat merusak sistem perbankan, mencuri data pribadi, dan menyebabkan kerugian finansial yang besar, semakin marak terjadi di seluruh dunia. Oleh karena itu, menjaga keamanan siber dalam sektor perbankan tidak hanya penting untuk melindungi data dan aset bank, tetapi juga untuk menjaga kepercayaan nasabah dan stabilitas ekonomi secara keseluruhan.

Sektor perbankan menghadapi berbagai tantangan dalam mengatasi ancaman siber yang terus berkembang. Salah satu tantangan utama adalah peran teknologi yang semakin canggih, yang memungkinkan penjahat siber untuk menciptakan metode baru dalam menyerang sistem perbankan. Selain itu, minimnya kesadaran mengenai pentingnya keamanan data baik di pihak bank maupun nasabah juga menjadi faktor yang memperburuk kondisi ini. Di sisi lain, perbankan harus tetap menjaga kelancaran operasional dan layanan kepada nasabah tanpa mengorbankan keamanan data yang mereka miliki. Seiring dengan tantangan-tantangan tersebut, sektor perbankan harus menemukan solusi inovatif untuk memperkuat keamanan siber. Solusi ini dapat mencakup penggunaan teknologi terkini, seperti kecerdasan buatan (AI) dan blockchain, serta penerapan kebijakan keamanan yang ketat. Selain itu, peningkatan kesadaran dan pelatihan kepada karyawan serta nasabah juga sangat penting untuk mencegah potensi ancaman yang datang dari kelalaian manusia.

Dalam era digital, berbagai bentuk ancaman siber seperti malware, phishing, ransomware, dan serangan Distributed Denial of Service (DDoS) terus berkembang dengan tingkat kompleksitas yang semakin tinggi. Pelaku kejahatan siber memanfaatkan celah keamanan dalam sistem perbankan untuk mencuri data, mengakses rekening, atau bahkan melumpuhkan layanan perbankan. Kondisi ini menjadi tantangan serius bagi perbankan dalam menjaga keamanan data dan sistem informasi yang menjadi tulang punggung operasional mereka.

Tantangan lain yang dihadapi adalah kebutuhan untuk menyeimbangkan inovasi teknologi dengan implementasi sistem keamanan yang andal. Sementara itu, faktor lain seperti kurangnya kesadaran karyawan dan nasabah terhadap praktik keamanan digital turut memperbesar risiko. Di sisi lain, regulasi yang dinamis dan kecepatan adopsi teknologi baru juga menuntut perbankan untuk terus beradaptasi dan mengembangkan strategi keamanan yang relevan.

Oleh karena itu, penting untuk mengidentifikasi tantangan-tantangan utama dalam keamanan siber perbankan dan mengeksplorasi solusi yang efektif. Dengan pendekatan yang komprehensif, mencakup penguatan teknologi, regulasi, serta edukasi pengguna, perbankan dapat meningkatkan sistem pertahanan mereka sekaligus menjaga kepercayaan publik. Penelitian ini bertujuan untuk membahas isu-isu tersebut serta menawarkan pandangan strategis dalam menghadapi ancaman keamanan siber di era digital.

KAJIAN TEORI

Keamanan siber dalam perbankan menjadi salah satu aspek kritis dalam era digital yang semakin maju. Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi dalam operasional perbankan, ancaman siber seperti pencurian data, malware, phishing, dan serangan ransomware menjadi tantangan utama. Teori keamanan informasi, seperti Confidentiality, Integrity, and Availability (CIA) Triad, menjadi landasan penting dalam memahami dan mengembangkan strategi untuk melindungi sistem perbankan. Teori ini menekankan pentingnya menjaga kerahasiaan informasi, memastikan integritas data, serta menjamin ketersediaan layanan perbankan bagi pengguna. Dalam konteks perbankan, teori trust dan perceived risk juga relevan untuk memahami bagaimana keamanan siber memengaruhi kepercayaan nasabah terhadap layanan digital. Tingkat kepercayaan nasabah sering kali bergantung pada kemampuan bank dalam menyediakan platform yang aman, melindungi data pribadi, dan merespons insiden siber secara efektif.

Penelitian sebelumnya menunjukkan bahwa implementasi teknologi seperti enkripsi data, firewall, dan sistem deteksi intrusi dapat membantu meningkatkan keamanan siber. Selain itu, literasi digital nasabah dan pelatihan karyawan menjadi solusi strategis untuk meminimalkan risiko human error yang sering kali menjadi celah dalam sistem keamanan. Tantangan lain yang sering dibahas adalah keterbatasan regulasi yang mengatur perlindungan data pribadi di beberapa negara, yang memerlukan sinergi antara pemerintah, sektor perbankan, dan pihak terkait. Dengan demikian, penelitian ini berlandaskan pada kombinasi teori keamanan informasi, kepercayaan nasabah, dan teknologi mitigasi ancaman siber. Pendekatan ini bertujuan untuk mengidentifikasi tantangan yang dihadapi sektor perbankan dalam era digital serta memberikan solusi yang praktis dan berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan studi literatur untuk menganalisis keamanan siber dalam sektor perbankan serta tantangan dan solusi yang dihadapi di era digital. Data yang digunakan dalam penelitian ini diperoleh melalui kajian terhadap buku, jurnal, artikel, dan sumber-sumber terpercaya lainnya yang relevan dengan topik keamanan siber, perbankan, serta teknologi digital. Studi literatur ini bertujuan untuk mengidentifikasi berbagai ancaman siber yang mengintai industri perbankan, menganalisis tantangan yang dihadapi oleh bank dalam mengimplementasikan sistem keamanan yang efektif, serta menggali solusi-solusi inovatif yang dapat digunakan untuk memperkuat pertahanan perbankan terhadap ancaman siber. Selain itu, penelitian ini juga mengandalkan analisis perbandingan terhadap praktik-praktik terbaik yang diterapkan oleh bank-bank di berbagai negara dalam menghadapi serangan siber. Analisis ini akan memberikan wawasan mengenai kebijakan dan teknologi yang dapat diterapkan di sektor perbankan untuk mengurangi risiko dan dampak dari ancaman siber. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan dan strategi keamanan siber yang lebih efektif dalam sektor perbankan di era digital. Melalui pendekatan kualitatif ini, penelitian bertujuan untuk menggali informasi secara mendalam dan menyajikan pemahaman yang lebih komprehensif mengenai tantangan dan solusi yang dapat dihadapi oleh sektor perbankan dalam menjaga keamanan sistem dan data mereka di tengah kemajuan teknologi digital.

HASIL PENELITIAN DAN PEMBAHASAN

1. Tingkat ancaman siber yang dihadapi sektor perbankan di era digital

Di era digital yang semakin maju, inovasi teknologi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor perbankan. Di Indonesia, sistem perbankan telah mengadopsi berbagai aplikasi dengan fitur-fitur terkini yang dirancang untuk memudahkan dan meningkatkan efisiensi dalam melakukan transaksi keuangan. Melalui electronic banking, nasabah kini dapat melakukan berbagai aktivitas perbankan hanya dengan beberapa klik di perangkat mereka. Fitur-fitur seperti pengecekan saldo, transfer dana antar rekening bank, dan pembayaran tagihan dapat dilakukan secara praktis dan cepat, tanpa harus mengunjungi bank secara fisik. Selain itu, aplikasi ini seringkali dilengkapi dengan fitur keamanan yang canggih, seperti autentikasi biometrik dan notifikasi transaksi, yang memberikan perlindungan tambahan bagi nasabah. Dengan kemudahan akses dan kecepatan layanan yang ditawarkan oleh teknologi ini, kehidupan sehari-hari masyarakat menjadi lebih efisien, memungkinkan mereka untuk mengelola keuangan dengan lebih baik dan menghemat waktu. Transformasi digital dalam perbankan tidak hanya meningkatkan kenyamanan bagi nasabah, tetapi juga mendorong inklusi keuangan dengan memberikan akses yang lebih luas kepada masyarakat untuk menggunakan layanan perbankan.

Berdasarkan data yang disampaikan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia mencapai sekitar 197,71 juta jiwa dari total populasi sekitar 266,91 juta penduduk. Angka ini menunjukkan bahwa sekitar 73,7% masyarakat Indonesia kini telah mampu mengakses internet. Peningkatan akses internet ini mencerminkan perkembangan teknologi informasi yang pesat di tanah air, yang memungkinkan lebih banyak individu untuk terhubung secara online. Dengan semakin banyaknya orang yang menggunakan internet, berbagai aspek kehidupan, termasuk pendidikan, bisnis, dan komunikasi, khususnya perbankan menjadi lebih terintegrasi dengan teknologi digital. Hal ini juga membuka peluang bagi inovasi dan pengembangan layanan digital yang dapat meningkatkan kualitas hidup masyarakat. Hal ini membuat adanya tuntutan secara tidak langsung kepada pihak perbankan untuk memberikan inovasi terbaru dalam sistem keuangan dalam bentuk mobile banking. Namun, pihak Bank juga harus memikirkan bagaimana cara memastikan keamanan data para nasabah agar aman sehingga tidak terjadi hal hal yang tidak diinginkan seperti tersebarnya data pribadi dan merusak kepercayaan nasabah.

Di sektor perbankan pada tahun 2023, aspek keamanan siber yang menjadi perhatian utama meliputi peningkatan serangan siber yang mencapai 43% menurut BSSN. Serangan ini mencakup berbagai bentuk, seperti malware dan phishing, yang mengancam integritas data dan operasional bank. Bank Indonesia telah menetapkan standar keamanan siber melalui PBI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran, namun pelaksanaannya masih terhambat oleh berbagai kendala teknis dan operasional.

Sebagai contoh kasus, pada tahun 2016 terjadi pencurian besar-besaran dari Bank Sentral Bangladesh yang melibatkan 81 juta dolar AS melalui rekening di New York Federal Reserve Bank. Pencurian ini berhasil dilakukan setelah peretas mengeksploitasi perangkat lunak Alliance Access SWIFT. Setelah insiden tersebut, serangan terkait juga dilaporkan terjadi di bank komersial di Vietnam, di mana malware digunakan untuk mengirim pesan SWIFT yang tidak sah dan menyembunyikan jejak transaksi yang mencurigakan. Dalam kasus lain, Banco del Austro (BDA) di Ekuador menggugat Wells Fargo setelah pencuri berhasil mentransfer 12 juta dolar AS dengan menggunakan pesan SWIFT yang mirip dengan permintaan transfer yang baru saja dibatalkan. BDA berargumen bahwa Wells Fargo seharusnya mendeteksi kejanggalan dalam

pesan tersebut, sementara Wells Fargo menyatakan bahwa kehilangan tersebut disebabkan oleh kredensial SWIFT yang sah yang dicuri dari karyawan BDA. Insiden-insiden ini menyoroti kerentanan dalam sistem transfer keuangan global dan pentingnya keamanan siber yang lebih ketat.

Pola penyerangan yang umum terjadi saat ini sering kali menargetkan pengguna atau nasabah yang melakukan transaksi melalui internet. Salah satu teknik yang banyak digunakan oleh para penyerang adalah phishing. Teknik phishing ini berfungsi untuk menyusup ke dalam jaringan dengan cara memanipulasi jalur data, sehingga penyerang dapat mengganti informasi yang seharusnya dengan data palsu. Melalui metode ini, penyerang dapat menciptakan situasi di mana korban menerima informasi yang tampak sah, tetapi sebenarnya telah dimanipulasi. Selain itu, teknik phishing juga dapat dimanfaatkan untuk menyebarkan malware. Para penyerang sering mengirimkan email yang berisi informasi terinfeksi kepada korban, yang dapat mengakibatkan sistem korban terinfeksi dan data sensitif mereka jatuh ke tangan yang salah. Dengan semakin canggihnya teknik-teknik ini, penting bagi pengguna untuk selalu waspada dan menerapkan langkah-langkah keamanan yang tepat saat bertransaksi secara online, agar terhindar dari ancaman yang merugikan.

Untuk mengurangi risiko serangan siber, lembaga perbankan dapat menerapkan sistem otentikasi dua faktor, yang berfungsi untuk memvalidasi data atau informasi yang akan diterima oleh nasabah. Sistem ini biasanya mencakup dua elemen otentikasi, yaitu penggunaan password yang diketahui oleh nasabah dan token, seperti smartcard atau aplikasi autentikasi yang menghasilkan kode unik. Dengan mengharuskan nasabah untuk memenuhi kedua persyaratan ini, perbankan dapat meningkatkan tingkat keamanan dalam proses transaksi. Tetapi untuk mencapai tingkat keamanan yang lebih tinggi, sangat disarankan agar bank juga menambahkan proses validasi biometrik. Metode biometrik, seperti pemindaian sidik jari, pengenalan wajah, atau pemindaian iris, dapat memberikan lapisan perlindungan tambahan yang sulit untuk dipalsukan atau dibobol. Dengan menggabungkan otentikasi dua faktor dengan teknologi biometrik, bank tidak hanya dapat melindungi data nasabah dengan lebih efektif, tetapi juga memberikan rasa aman yang lebih besar bagi nasabah saat melakukan transaksi. Hal ini sangat penting di era digital saat ini, di mana ancaman terhadap keamanan informasi semakin meningkat dan nasabah perlu merasa yakin bahwa data mereka terlindungi dengan baik.

Tingkatan serangan siber yang terjadi khususnya di Indonesia bukan hanya menjadi permasalahan nasional. Namun, permasalahan ini cukup mendunia dan seringkali terjadi tanpa adanya penanganan yang cepat dan tepat sehingga sulit untuk mempertahankan data tanpa adanya kebocoran yang masif.

2. Tantangan Utama yang Dihadapi Oleh Perbankan dalam Menerapkan Sistem Keamanan Siber yang Efektif

Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, memungkinkan peningkatan efisiensi operasional dan kemudahan bagi nasabah. Namun, transformasi ini juga menghadirkan tantangan baru, terutama dalam hal keamanan siber. Ancaman siber yang semakin kompleks dan canggih, seperti pencurian data, ransomware, dan serangan Distributed Denial of Service (DDoS), menjadi perhatian utama dalam menjaga integritas sistem perbankan. Perbankan tidak hanya harus melindungi data nasabah yang sensitif, tetapi juga memastikan kelancaran layanan operasional untuk mencegah kerugian finansial dan reputasi.

a) Serangan Phishing dan Social Engineering

Serangan Phishing dan Social Engineering adalah tantangan signifikan dalam keamanan siber industri perbankan karena memanfaatkan faktor kelemahan manusia. Phishing dilakukan dengan mengelabui korban agar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya melalui email, pesan teks, atau situs web palsu. Dalam konteks perbankan, serangan ini sering menyasar nasabah untuk mendapatkan akses ke rekening bank mereka. Tingginya tingkat kepercayaan nasabah terhadap komunikasi resmi bank menjadi celah bagi pelaku untuk membuat serangan mereka tampak meyakinkan. Phishing juga sering dikombinasikan dengan teknik lain, seperti malware, untuk meningkatkan efektivitas serangan.

Teknik Social Engineering memanfaatkan psikologi manusia, seperti rasa takut atau kepanikan, untuk memanipulasi individu agar mengambil tindakan tertentu yang menguntungkan pelaku serangan. Contohnya adalah telepon palsu yang mengaku dari bank dan meminta informasi rahasia atas nama "keamanan akun". Serangan ini sangat sulit dideteksi karena tidak hanya bergantung pada kerentanan teknis tetapi juga pada kelemahan emosional manusia. Dalam industri perbankan, serangan phishing dan social engineering menjadi ancaman utama karena dampaknya dapat mencakup pencurian identitas, pengurasan dana, dan kerugian reputasi yang serius bagi bank.

b) Malware dan Ransomware

Dalam industri perbankan, malware dan ransomware merupakan tantangan signifikan bagi keamanan siber karena dampaknya yang luas terhadap operasional dan reputasi. Malware sering digunakan untuk mencuri data sensitif seperti informasi pelanggan atau kredensial login. Dalam konteks perbankan, serangan semacam ini menjadi lebih kompleks karena pelaku kejahatan siber mengadopsi teknik seperti trojan perbankan yang dapat menargetkan transaksi keuangan secara langsung. Ancaman ini semakin parah dengan peningkatan adopsi teknologi keuangan (FinTech) yang sering kali memperluas permukaan serangan dengan banyaknya interkoneksi antar sistem. Implementasi langkah-langkah pencegahan seperti autentikasi multifaktor (MFA) dan pengawasan ketat akses data menjadi solusi yang sering diterapkan untuk mengurangi risiko ini.

Ransomware, di sisi lain, menonjol sebagai ancaman yang mengunci akses ke sistem penting dan sering kali diiringi dengan tuntutan tebusan besar. Dalam industri keuangan, serangan ransomware tidak hanya mengganggu operasional tetapi juga dapat membahayakan data pelanggan yang disandera atau diekspos. Strategi mitigasi yang direkomendasikan termasuk pengelolaan backup data yang solid, implementasi kontrol akses berbasis prinsip least-privileged, dan pelaporan insiden kepada otoritas seperti FBI, yang dapat membantu mengurangi dampak serangan. Selain itu, bank juga didorong untuk meningkatkan kebijakan tata kelola data dan pengawasan siber guna memenuhi persyaratan regulasi yang terus berkembang.

c) Serangan DDoS (*Distributed Denial of Service*)

Serangan DDoS (Distributed Denial of Service) adalah salah satu ancaman terbesar dalam keamanan siber, terutama bagi sektor perbankan. Serangan ini melibatkan membanjiri server atau jaringan dengan lalu lintas palsu, sehingga mengganggu layanan yang sah. Dalam konteks perbankan, serangan DDoS sering kali bertujuan untuk melumpuhkan situs web atau aplikasi layanan pelanggan, menghalangi transaksi penting, atau bahkan mengalihkan perhatian dari serangan lain yang lebih merusak, seperti pencurian data atau ransomware. Kompleksitas serangan ini meningkat seiring dengan pemanfaatan perangkat botnet yang

tersebar secara global, menjadikannya sulit untuk dibedakan dari lalu lintas sah. Akibatnya, institusi perbankan sering menghadapi risiko kerugian finansial yang signifikan, termasuk biaya mitigasi dan kerusakan reputasi.

Selain dampaknya terhadap layanan pelanggan, serangan DDoS memengaruhi kepercayaan publik terhadap keamanan sistem perbankan. Teknologi berbasis cloud yang semakin banyak diadopsi sektor perbankan juga menjadi target utama karena kerentanannya terhadap kelebihan kapasitas jaringan. Sementara solusi seperti deteksi berbasis machine learning atau blockchain mulai diterapkan untuk mitigasi, upaya ini masih menghadapi tantangan teknis dan kebutuhan sumber daya yang besar. Strategi keamanan proaktif, termasuk pemantauan jaringan secara real-time dan pengujian ketahanan, menjadi kunci untuk mengurangi ancaman DDoS di masa depan.

d) Keterbatasan Sumber Daya dan Keterampilan

Dalam sektor perbankan, keterbatasan sumber daya dan kekurangan tenaga ahli menjadi tantangan utama dalam memastikan keamanan siber yang memadai. Institusi keuangan harus melindungi data sensitif dalam jumlah besar, tetapi sering kali menghadapi keterbatasan anggaran dan sumber daya manusia. Hal ini menjadi masalah yang signifikan mengingat ancaman siber terus berkembang. Institusi kecil, khususnya, kesulitan untuk mengikuti langkah-langkah keamanan yang diperlukan karena kurangnya dana untuk menginvestasikan teknologi terbaru serta kekurangan keahlian untuk menerapkannya secara efektif. Selain itu, mereka juga dihadapkan pada tekanan besar untuk mematuhi regulasi yang kompleks terkait perlindungan data dan privasi.

Salah satu aspek penting dari masalah ini adalah kesenjangan keterampilan dalam keamanan siber, yang sangat dirasakan di industri perbankan. Seiring dengan semakin canggihnya ancaman siber, permintaan terhadap profesional keamanan siber yang berkualitas terus melebihi pasokan. Banyak institusi keuangan, terutama yang lebih kecil, kesulitan merekrut dan mempertahankan talenta dengan keahlian yang diperlukan untuk menangani ancaman ini. Meski kebutuhan terus meningkat, sistem pendidikan belum sepenuhnya menyesuaikan dengan tuntutan yang berubah di bidang keamanan siber, sehingga terjadi ketidaksesuaian antara keterampilan yang tersedia dan kebutuhan industri. Program seperti Cybersecurity Workforce Alliance berupaya menjembatani kesenjangan ini dengan menciptakan jalur yang lebih efektif antara dunia akademik dan sektor perbankan, tetapi tantangan besar masih ada.

e) Regulasi dan Kepatuhan

Kepatuhan terhadap regulasi menjadi tantangan besar dalam keamanan siber di industri perbankan, khususnya dalam menghadapi perubahan undang-undang dan standar yang terus berkembang. Regulator di seluruh dunia kini menyesuaikan kerangka kerja mereka untuk menangani ancaman siber yang semakin kompleks, dengan fokus pada perlindungan kerahasiaan, integritas, dan ketersediaan sistem keuangan. Namun, sering kali terdapat kesenjangan antara kepatuhan teoretis dengan hasil keamanan yang nyata. Hal ini terjadi ketika lembaga keuangan hanya memenuhi persyaratan minimum regulasi tanpa memastikan bahwa langkah-langkah keamanan mereka benar-benar tangguh, sehingga menciptakan celah dalam sistem. Misalnya, meskipun regulasi seperti GDPR dan ISO 27001 mewajibkan penilaian risiko dan kontrol keamanan, penelitian menunjukkan bahwa kepatuhan saja tidak selalu meningkatkan performa keamanan secara signifikan.

Selain itu, keragaman regulasi di berbagai wilayah menambah kompleksitas kepatuhan bagi bank internasional. Penerapan undang-undang seperti regulasi keamanan siber oleh New York Department of Financial Services atau PSD2 di Uni Eropa menciptakan lanskap regulasi yang terfragmentasi. Bank harus menavigasi persyaratan yang berbeda ini sambil menyeimbangkan biaya kepatuhan dengan kebutuhan untuk menerapkan strategi keamanan siber yang efektif. Ketidaksesuaian antara praktik kepatuhan dan keamanan yang sebenarnya dapat merusak efektivitas keduanya, karena organisasi mungkin terlalu berfokus pada pemenuhan kewajiban hukum tanpa benar-benar mengatasi risiko keamanan mendasar. Seiring meningkatnya ancaman keamanan siber, regulator semakin menekankan integrasi kerangka kerja keamanan siber dan manajemen risiko untuk memberikan perlindungan yang lebih komprehensif di sektor keuangan.

Industri perbankan menghadapi tantangan besar dalam melawan ancaman siber, seperti phishing, ransomware, hingga pelanggaran data. Untuk mengatasi hal ini, bank harus menerapkan pendekatan multi-lapis yang mencakup pemanfaatan teknologi canggih dan kebijakan keamanan yang ketat. Salah satu solusi utama adalah adopsi teknologi seperti kecerdasan buatan (AI) untuk mendeteksi dan merespons ancaman secara real-time. Selain itu, penggunaan autentikasi multifaktor (MFA) dan pendekatan "zero-trust network architecture" (ZTNA) dapat memperkuat kontrol akses dan melindungi data pelanggan. Program pelatihan kesadaran siber juga menjadi langkah penting untuk mengurangi risiko dari ancaman yang melibatkan kesalahan manusia.

Dari sisi regulasi, bank perlu mematuhi standar keamanan global seperti Payment Card Industry Data Security Standard (PCI DSS) dan membangun kerangka kerja kolaboratif dengan institusi keuangan lainnya. Selain itu, pengawasan ketat terhadap vendor pihak ketiga menjadi penting karena banyak pelanggaran data terjadi melalui kelemahan dalam rantai pasokan. Untuk mitigasi risiko sistemik, lembaga seperti Financial Systemic Analysis & Resilience Center (FSARC) membantu mengidentifikasi titik lemah pada sistem keuangan yang dapat memperbesar dampak serangan. Pendekatan ini, jika dilakukan secara konsisten, dapat meningkatkan ketahanan sektor perbankan terhadap ancaman siber yang terus berkembang.

KESIMPULAN

Kemajuan teknologi digital telah membawa transformasi besar dalam sektor perbankan, memberikan kemudahan dan efisiensi layanan yang signifikan. Namun, inovasi ini juga disertai dengan tantangan besar, terutama terkait keamanan siber. Tingginya ancaman siber seperti phishing, malware, ransomware, dan serangan DDoS menjadi tantangan utama yang dihadapi sektor perbankan, yang tidak hanya mengancam data sensitif nasabah tetapi juga stabilitas operasional lembaga keuangan. Kompleksitas serangan, keterbatasan sumber daya, rendahnya kesadaran keamanan, serta keragaman regulasi memperumit upaya untuk menciptakan sistem keamanan siber yang tangguh. Solusi yang efektif membutuhkan pendekatan multi-lapis yang mencakup penerapan teknologi canggih seperti kecerdasan buatan (AI), blockchain, dan sistem autentikasi multifaktor (MFA), serta edukasi intensif kepada karyawan dan nasabah untuk meningkatkan kesadaran terhadap keamanan siber. Selain itu, harmonisasi regulasi dan pengawasan ketat terhadap vendor pihak ketiga menjadi aspek penting dalam memitigasi risiko yang muncul.

DAFTAR PUSTAKA

Ardianto, R., Ramdhani, R. F., Dewi, L. O. A., Prabowo, A., Saputri, Y. W., Lestari, A. S., & Hadi, N. (2024). Transformasi digital dan antisipasi perubahan ekonomi global dalam dunia perbankan. *MARAS: Jurnal Penelitian Multidisiplin, 2*(1), 80-88.

Asosiasi Penyelenggara Jasa Internet Indonesia. (n.d.). Survei APJII: Pengguna internet di Indonesia tembus 215 juta orang.

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa023

Dembosky, L., & Kelly, J. R. (2024). Ransomware in the financial sector. *ABA Risk and Compliance Magazine, September-October 2024.* https://bankingjournal.aba.com/2024/08/ransomware-in-the-financial-sector/

EC-Council University. (n.d.). Why is cybersecurity important in the financial industry?. Diakses pada 2 Desember 2024.

EC-Council University. (2024). Cybersecurity threats and countermeasures in the banking industry.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam, 5*(2), 87-100.

Falowo, O. I., & Bou Abdo, J. (2024). 2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques. *IEEE Access, 12*, 26759–26771. https://doi.org/10.1109/ACCESS.2024.3367240

Fatima, A. (2011). E-banking security issues-Is there a solution in biometrics?. *Journal of Internet Banking and Commerce, 16*(2), 1.

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital, 1*(2), 57-61.

Gupta, A., & Paramesh, K. (2021). A Novel Symmetry-Based Framework for Optimization Problems. *Symmetry, 13*(2), 227. https://doi.org/10.3390/sym13020227

Healey, J., Mosser, P., Rosen, K., & Tache, A. (2018). The future of financial stability and cyber risk. *Brookings.* Diakses pada 2 Desember 2024, dari https://www.brookings.edu/articles/the-future-of-financial-stability-and-cyber-risk/

Jo Ann Barefoot. (2020). Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech. *Mossavar-Rahmani Center for Business & Government Associate Working Paper Series No. 151*. Harvard Kennedy School.

Marotta, A., & Madnick, S. (2020). Analyzing the interplay between regulatory compliance and cybersecurity (CISL# 2020-06). *Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute*

of Technology. https://doi.org/10.2139/ssrn.3479012

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik, 1*(2), 60-65.

Styarini, F., & Riptiono, S. (2020). Analisis pengaruh customer trust terhadap keputusan menggunakan mobile banking melalui perceived risk dan perceived usefulness sebagai variabel intervening. *Jurnal Ilmiah Mahasiswa Manajemen, Bisnis Dan Akuntansi (JIMMBA, 2*(4), 670-680.

Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya – Kompaspedia. (2024, July 30). *Kompaspedia.* https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya

Wang, C., Ahmad, S. F., Ayassrah, A. Y. B. A., Awwad, E. M., Irshad, M., Ali, Y. A., & Han, H. (2023). An empirical evaluation of technology acceptance model for Artificial Intelligence in E-commerce. *Heliyon, 9*(8).

Wardani, A. S. (2016, June 22). Bank Sentral Bangladesh Dibobol Hacker, Rp 1,06 Triliun Ludes. *Liputan6.* https://www.liputan6.com/tekno/read/2462290/bank-sentral-bangladesh-dibobol-hacker-rp-106-triliun-ludes

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Boston: Cengage Learning.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive, 12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Buku Teks

Raharja, A. R., ST, M., & Kom, M. (2024). *Keamanan Jaringan.* Penerbit Kbm Indonesia.