Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 9, No. 10, Oktober 2024

SERANGAN SIBER DALAM PERKEMBANGAN PERBANKAN DIGITAL DI INDONESIA

Ilham Zharfan Satrya
Universitas Padjajaran, Bandung, Indonesia
Email: ilham23010@mail.unpad.ac.id

Abstrak

Pesatnya kemajuan teknologi informasi telah membawa era baru dalam masyarakat global yang biasa disebut dengan "Revolusi Industri 4.0". Pergeseran perilaku konsumen ke arah platform digital menyebabkan perbankan mempercepat proses transformasi menjadi bank digital. Perkembangan digital banking bersama dengan seluruh infrastrukturnya pasti akan menimbulkan tantangan khusus dalam tranformasi bank digital di masa depan. Di era teknologi dan disrupsi digital, salah satu hal yang harus diwaspadai adalah kemungkinan serangan siber. Penulisan ini memaparkan pemikiran secara kritis mengenai dampak serangan keamanan siber dalam perkembangan perbankan digital di Indonesia dan strategi mitigasi efektif dalam menangani serangan keamanan siber. Penulisan ini mengelaborasi menggunakan pendekatan studi literatur untuk mengidentifikasi perkembangan perbankan digital di Indonesia, serangan keamanan siber dan dampaknya bagi perbankan, dan strategi pencegahan efektif untuk mengatasi serangan keamanan siber. Penulisan ini diharapkan dapat memberikan wawasan baru untuk perbankan digital di Indonesia dalam mengetahui jenis serangan siber dan menangani serangan keamanan siber dengan strategi pencegahan yang efektif. Nasabah dan pihak perbankan harus memiliki kesadaran keamanan siber dalam hal transaksi antar pihak dalam perbankan digital. Penulisan ini memaparkan berbagai cara dalam memberikan solusi serangan keamanan siber dan jenis – jenis serangan keamanan siber yang harus diwaspadai.

Kata kunci: Perkembangan Perbankan Digital, Serangan Keamanan Siber, Nasabah

Abstract

The rapid advancement of information technology has brought a new era in global society commonly referred to as the "Industrial Revolution 4.0". The shift in consumer behavior towards digital platforms has caused banks to accelerate the transformation process into digital banks. The development of digital banking along with all its infrastructure will definitely pose special challenges in the transformation of digital banks in the future. In the era of technology and digital disruption, one of the things to watch out for is the possibility of cyberattacks. This paper presents critical thinking about the impact of cybersecurity attacks on the development of digital banking in Indonesia and effective mitigation strategies in dealing with cybersecurity attacks. This paper elaborates using a literature study approach to identify the development of digital banking in Indonesia, cybersecurity attacks and their impact on banks, and effective prevention strategies to overcome cybersecurity attacks. This paper is expected to provide new insights for digital banking in Indonesia in knowing the types of cyber attacks and dealing with cyber security attacks with effective prevention strategies. Customers and banks must have cybersecurity awareness in terms of transactions between parties in digital banking. This paper explains various ways to provide cybersecurity attack solutions and the types of cybersecurity attacks that must be watched out for.

Keywords: *Perkembangan Perbankan Digital, Serangan Keamanan Siber, Nasabah*

How to cite:	Satrya, I. Z. (2024). Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia. *Syntax Literate. (9)10.* http://dx.doi.org/10.36418/syntax-literate.v9i10
E-ISSN:	2548-1398

Pendahuluan

Pesatnya kemajuan teknologi informasi telah membawa era baru dalam masyarakat global yang biasa disebut dengan "Revolusi Industri 4.0" (Purba et al., 2021). Pemanfaatan berbagai teknologi dalam bidang jasa keuangan telah membawa perubahan yang signifikan pada industri perbankan (Al Qardh et al., 2019). Pergeseran perilaku konsumen ke arah platform digital menyebabkan perbankan mempercepat proses transformasi menjadi bank digital (Hill, 2021). Secara keseluruhan, transaksi digital global pada tahun 2017 hingga 2021 meningkat sebesar 118%, dari USD 3,09 triliun pada tahun 2017 menjadi USD 6,75 triliun pada tahun 2021 (Statista, 2021). Di Indonesia, tingkat pertumbuhan transaksi digital telah mencapai angka tertinggi sepanjang masa, yaitu sebesar 1,556 persen pada kuartal terakhir tahun 2017–2020. Pada tahun 2021, transaksi mata uang elektronik mencapai Rp786,35 triliun. Pendapatan tahun ini melampaui Rp281,39 triliun (55,73%) dibandingkan total pendapatan tahun sebelumnya hanya Rp504,96 triliun (Bank Indonesia, 2021).

Berdasarkan laporan Bank Indonesia, selama triwulan III tahun 2023, nilai transaksi Uang Elektronik (UE) meningkat 10,34% (yoy) mencapai Rp116,54 triliun, sedangkan nilai transaksi perbankan digital mencapai Rp15.148,71 triliun, naik sebesar 12,83% (yoy). Alhasil, nilai nominal transaksi QRIS mencapai Rp56,92 triliun dan meningkat 87,90% (yoy) dengan 41,84 juta pengguna dan 29,04 juta merchant yang mayoritas merupakan UMKM. Bank Indonesia terus mendorong digitalisasi sistem pembayaran dan persyaratan kerja dengan sistem pembayaran asing untuk meningkatkan pemahaman ekonomi keuangan dan mata uang digital. Namun perlu dicatat, persentase pembayaran melalui ATM, bank, dan kartu kredit hanya meningkat 4,94 persen (yoy) menjadi Rp2.041,72 triliun dibandingkan triwulan sebelumnya. Bagaimanapun, masyarakat modern semakin bergantung pada layanan perbankan digital yang dapat digunakan di mana saja. (Bank Indonesia, 2021)

Laju perbankan digital di Indonesia terhambat oleh berbagai faktor yang menghambat perkembangan bank digital di tanah air, padahal Indonesia merupakan negara dengan perekonomian yang sangat potensial dalam hal digitalisasi (Sriekaningsih, 2020). Faktor pendorong tersebut dievaluasi dalam tiga aspek utama: peluang digital, perilaku digital, dan transaksi digital. Potensi digital mencakup namun tidak terbatas pada potensi demografi, potensi ekonomi dan digital, potensi penetrasi pengguna internet, dan potensi pertumbuhan konsumen (Ardianto et al., 2024). Kesenjangan digital terdiri dari kepemilikan ponsel cerdas dan penggunaan aplikasi seluler. Transaksi digital meliputi pembelian online (e-commerce), perbankan digital, dan transfer uang elektronik (Wulandari, 2023). Jika dibandingkan dengan potensi yang dimanfaatkan oleh industri perbankan, transformasi digital menimbulkan tantangan yang perlu diatasi. Beberapa risiko tersebut antara lain perlindungan privasi dan kehilangan data, risiko investasi teknologi yang tidak sejalan dengan strategi bisnis, risiko kecerdasan buatan, risiko siber, dan perlunya manajemen risiko kelembagaan yang berorientasi digital, literasi digital yang masih relatif rendah. infrastruktur teknologi informasi yang rendah dan belum berkembang di Indonesia, dan mitigasi risiko peraturan (ISACA, 2022).

Oleh karena itu, risiko – risiko tersebut harus dimitigasi seiring dengan berjalanya perkembangan digital banking. Perkembangan digital banking bersama dengan seluruh infrastrukturnya pasti akan menimbulkan tantangan khusus dalam tranformasi bank digital di masa depan. Di era teknologi dan disrupsi digital, salah satu hal yang harus diwaspadai adalah kemungkinan serangan siber. Sangat disadari bahwa penggunaan teknologi informasi secara masif meningkatkan risiko serangan siber, yang juga dapat

menyebabkan kebocoran atau pencurian data pelanggan. Bank juga harus mempertimbangkan risiko yang belum pernah terjadi sebelumnya, seperti risiko kegagalan keamanan dan sistem, blackout digital, dan potensi kerusakan sistemik akibat bank run digital. (Sesi 6 POJK+11-POJK.03-2022+Penyelenggaraan Teknologi Informasi Oleh Bank Umum+FAQ, 2022.).

Dalam hal kemungkinan serangan siber, sektor keuangan, khususnya perbankan, adalah yang paling rentan terhadap serangan siber, menurut data dari Badan Siber dan Sandi Negara (BSSN). Serangan yang paling umum termasuk phishing dan ransomware. Oleh karena itu, bank harus melakukan berbagai upaya untuk mempertahankan ketahanan dan keamanan siber secara konsisten untuk meningkatkan resistensi mereka terhadap berbagai pola serangan siber baru. Beberapa upaya yang dapat dilakukan oleh bank antara lain dengan melakukan pengujian keamanan siber, menilai kemampuan keamanan siber secara mandiri, dan melaporkan insiden siber. Selain itu, peningkatan teknologi menyebabkan peningkatan penggunaan pihak ketiga, yang berpotensi menimbulkan risiko tambahan pada aktivitas bank, seperti risiko operasional. Selain itu, kemajuan teknologi harus diimbangi oleh kesiapan organisasi, termasuk pemimpin dan talenta digital yang cukup, baik secara kuantitas maupun kualitas, budaya organisasi yang berorientasi digital, dan desain organisasi yang mendukung transformasi digital. (Laporan Tahunan Monitoring Keamanan Siber 2021, 2022).

Berdasarkan permasalahan tersebut, penulisan ini menekankan bahwa sangat penting untuk mengidentifikasi jenis serangan siber dan dampaknya pada perkembangan perbankan digital di Indonesia serta membuat solusi mitigasi yang lebih baru dan efektif dalam mengatasi serangan siber tersebut.

Metode Penelitian

Dalam penelitian ini, pendekatan kualitatif digunakan untuk melihat kondisi alami fenomena. Penelitian kualitatif bertujuan untuk memahami fenomena yang dialami oleh subjek penelitian secara menyeluruh, seperti perilaku, persepsi, motivasi, tindakan, dll., secara eksplisit dan menggunakan berbagai metode ilmiah dalam lingkungan alami (Muhammad et al., 2023). Tujuan dari penelitian deskriptif-kualitatif ini adalah untuk mengidentifikasi pemikiran di balik Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia.

Dalam penelitian ini, paradigma kritis digunakan sebagai sudut pandang, acuan, dan dimensi waktu untuk memahami fenomena selama proses penelitian (Muhammad et al., 2023). Dalam penelitian ini, paradigma kritis yang digunakan adalah perspektif penelitian sosial alternatif. Tujuan dari perspektif ini adalah untuk mengkritik dan membela keadaan saat ini serta memberikan informasi yang berbeda untuk membangun tatanan sosial yang lebih baik. Pilihan paradigma kritis disesuaikan dengan teori dan subjek penelitian yang menggunakan pendekatan kritis. Hal ini disebabkan oleh fakta bahwa fokus penelitian ini adalah untuk mempelajari kelemahan keamanan siber yang terjadi selama kemajuan perbankan digital di Indonesia.

Analisis Isi Konten Kritis (CCA) adalah pendekatan konseptual untuk memahami apa itu teks dengan mempertimbangkan studi sosiohistoris, gender, budaya, atau tematik (Muhammad et al., 2023). CCA berfokus pada bagaimana teks (termasuk aspek visual dan linguistik) dapat digunakan untuk mengidentifikasi ide, nilai, identitas, dankekuatan tersembunyi dalam menyampaikan materi. Untuk penelitian yang mempelajari teks, analisis isi konten kritis adalah metode yang fleksibel dalam hal pendekatan teoretis dan pemilihan teks. Dalam penelitian ini, peneliti tertarik untuk menganalisis serangan siber

dalam perkembangan perbankan digital di Indonesia. Penelitian ini berbeda dari penelitian sebelumnya karena peneliti menawarkan pengembangan konten dengan menambahkan strategi mitigasi yang efektif untuk mengatasi serangan siber yang berdampak pada pertumbuhan perbankan digital di Indonesia.

Alat ukur penelitian ini dibuat dengan mempelajari metode studi literatur dari berbagai sumber, yang menghasilkan istilah khusus untuk setiap dimensi. Peneliti melakukan proses pengumpulan data seperti membaca buku atau dokumen, mengumpulkan beberapa jurnal dan artikel, dan meneliti tentang Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia. Alat ukur ini merujuk pada literatur berikut: (OJK, 2021), (Bangkitnya Era Perbankan Digital, 2021), (Aripin et al., 2022), (Mamun & Ningsih, 2021), (Akinbowale et al., 2024a), (Chhabra Roy & Prabhakaran, 2023), (Chhabra Roy & P, 2024), (Akinbowale et al., 2024), (Cele & Kwenda, 2024), (Hill, 2021), dan (ISACA, 2022). Literatur – literatur tersebut diperoleh untuk mengkaji dampak serangan siber dalam perbankan digital dan solusi mitigasi yang efektif dalam pencegahan serangan siber tersebut.

Hasil dan Pembahasan

Serangan Risiko Siber dan Implikasinya pada Perkembangan Perbankan Digital di Indonesia

Berdasarkan konten (OJK, 2021), Dalam hal kejahatan siber, perilaku yang melanggar hukum yang dikendalikan melalui operasi elektronik yang menargetkan sistem keamanan komputer dan data yang diproses. Sumber daya manusia (SDM) dapat menjadi sumber risiko siber dalam bentuk ketidakmampuan SDM untuk melaksanakan tugas yang berkaitan dengan pengamanan aset dan informasi bank atau kurangnya kesadaran keamanan SDM dalam melaksanakan tugas dan proses kerja sehari-hari, serta faktor lain yang berkaitan dengan integritas SDM bank. Proses bisnis yang dirancang dan dijalankan oleh bank dapat menyebabkan risiko siber bagi bank. Kelemahaan dalam proses ini antara lain dapat mencakup tidak menggunakan channel transmisi yang aman, tidak melakukan audit aspek keamanan secara berkala, manajemen password yang buruk, dan penggunaan internet publik yang tidak aman. Kelemahan pada teknologi informasi dan infrastruktur Bank dapat menjadi sumber risiko siber. Kurangnya pengujian pengamanan, kontrol, dan monitoring ancaman dan kerentanan, kelemahan sistem, seperti tidak tersedianya anti *malware*/ anti-virus, dan sistem yang tidak update menjadi jalan bagi masuknya risiko siber kepada Bank. Faktor eksternal yang paling signifikan yang menyebabkan risiko siber bagi bank adalah kesadaran keamanan nasabah yang rendah dan peningkatan strategi dan kemampuan pelaku serangan siber.

Ancaman Keamanan Siber pada perkembangan perbankan digital di Indonesia mencakup Penyusupan (*intrusion*) adalah ketika seseorang memasuki sistem dan aplikasi Bank tanpa izin dan sepengetahuan Bank dan berusaha untuk mengubah sistemnya. Penyusupan dapat menyerang sistem dengan menggunakan identifikasi pengguna yang sah dan parameter koneksi seperti sandi, atau dengan menggunakan kerentanan yang ada pada sistem dan aplikasi. Salah satu teknik utama yang digunakan untuk mendapatkan akses ke dalam sistem dan aplikasi adalah menebak sandi yang digunakan (*brute force*), mengakses akun yang tidak dilindungi dengan sandi, melakukan penipuan atau rekayasa sosial, mendengarkan lalu lintas komunikasi data dengan alat penyadap, memasukkan program mata-mata (*spyware*) atau program kecil yang biasanya digunakan sebagai pengganti diri untuk masuk ke dalam sistem dan aplikasi (*trojan horse*), mengakses file untuk menyimpan sandi yang dienkripsi dalam jaringan untuk menguji seluruh penetrasi

dalam pemecahan sandi. Serangan phishing dilakukan dengan menggunakan alamat web palsu yang memiliki tampilan yang sama dengan website asli. Tujuan dari serangan phishing ini adalah untuk mendapatkan informasi sensitif seperti *username* dan *password*. *Malware* adalah program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal sistem komputer. Program *malware* biasanya dibuat untuk mendapatkan keuntungan finansial atau keuntungan lainnya. Jumlah serangan malware terus meningkat, menjadikannya pandemi yang sangat nyata saat ini. *Malware* telah menyebar di mana-mana dan berdampak pada semua orang yang bekerja dalam setiap bidang bisnis. Setiap program komputer berbahaya yang memiliki kemampuan untuk mereplikasi dan menyebarkan dirinya sendiri disebut virus generic (OJK, 2021).

Dalam kebanyakan kasus, *Denial of Service (DoS) dan Distributed Denial of Service (DDoS)* memanfaatkan kapasitas sistem yang berlebihan, memaksa pengguna yang sah untuk tidak dapat mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Tujuan dari serangan ini adalah untuk mengganggu operasi sistem dengan memaksa sistem untuk menerima jumlah akses dan proses yang lebih besar daripada yang dapat ditangani. sehingga sistem menjadi terlalu sibuk dan crash, menyebabkan ketidakmampuan untuk melayani atau beroperasi. Permasalahan ini membahayakan bank yang bergantung sepenuhnya pada kemampuan internet untuk menjalankan operasinya. Serangan defacement, yang dilakukan dengan mengganti atau mengubah halaman web korban sehingga kontennya berubah sesuai dengan niat penyerang. Serangan spam, dilakukan dengan mengirimkan email yang tidak dikehendaki untuk tujuan komersial atau publisitas, memasang perangkat lunak berbahaya, atau membuat server penuh dengan beban. Mengabaikan Protokol Komunikasi Sebuah serangan spoofing Transmision Control Protocol (TCP) bergantung pada fakta bahwa protokol TCP menetapkan koneksi logis antara dua ujung sistem untuk mendukung pertukaran data. Untuk membangun koneksi ini, pengidentifikasi logis, atau nomor port, digunakan. Sebuah serangan nomor port TCP akan melibatkan proses menebak atau memprediksi nomor port berikutnya yang akan diberikan untuk pertukaran data dengan menggunakan angka bukan pengguna yang Ini memungkinkan hacker dan target untuk melewati firewall dan membangun hubungan yang aman (OJK, 2021).

Sosial engineering berarti mendapatkan informasi pelanggan seperti PIN, nomor baru, atau informasi lainnya dengan menghubungi pelanggan melalui telepon, SMS, atau media lain untuk memberi tahu pelanggan informasi tertentu untuk menghubungi nomor atau situs web tertentu. Bisnis email *compromise* adalah kejahatan siber social engineering yang memanfaatkan celah kerentanan email yang menargetkan individu, perusahaan, dan profesional. Mereka memanfaatkan akun email pribadi atau bisnis untuk mengirimkan instruksi pembayaran palsu dan informasi lain yang digunakan untuk melakukan penipuan keuangan. Dampak dari serangan risiko siber pada perkembangan perbankan digital di Indonesia yaitu kerugian yang dapat dihitung dan berdampak langsung pada bank disebut kerugian langsung. Contohnya adalah kehilangan aset dan pembayaran ganti rugi kepada nasabah. Kerugian tidak langsung adalah kerugian yang sulit dihitung secara kuantitatif, tetapi dapat mengurangi efisiensi operasional bank. Contoh kerugian tidak langsung termasuk proses kerja yang tidak efisien, kehilangan peluang untuk memperoleh klaim atau keuntungan, dan kehilangan atau menurunkan kepercayaan masyarakat terhadap bank (OJK, 2021).

Dalam penelitian sebelumnya oleh (Cele & Kwenda, 2024), menemukan dan menyelidiki 17 ancaman keamanan siber yang berbeda yang memengaruhi penggunaan perbankan digital dengan menggunakan metode SLR. Pencurian identitas, serangan

malware, phishing, dan vishing muncul sebagai salah satu ancaman yang paling signifikan yang menghalangi penggunaan layanan perbankan digital dengan lancar. Korban bahaya ini biasanya menunjukkan keengganan tertentu untuk menggunakan platform perbankan digital yang mudah. Penelitian oleh (Akinbowale et al., 2024) menunjukkan bahwa penipuan siber memiliki dampak yang cukup besar pada industri perbankan Afrika Selatan. Hasil menunjukkan bahwa jenis penipuan siber yang paling umum dilakukan di industri perbankan Afrika Selatan meliputi phishing, mata-mata, malware, pencurian data, pencurian uang, dan hilangnya pemegang saham.

Strategi Pengendalian Risiko Siber pada Perkembangan Perbankan Digital di Indonesia

OJK mengungkapkan di dalam kontennya bahwa risiko siber pada perkembangan perbankan digital di Indonesia perlu diatasi dengan memuat bagaimana Bank menetapkan toleransi risiko keamanan siber dan tata cara Bank mengidentifikasi, mengurangi, dan mengelola risiko keamanan siber untuk mencapai keamanan siber. Bank memuat pokok-pokok prinsip manajemen keamanan siber ini, antara lain terkait *governance, strategy, identification, protection, vigilance, resilience, and internal control system* memuat rencana kelangsungan usaha (*business continuity plan atau business continuity management*) atas kemungkinan kondisi eksternal dan internal terburuk dari serangan keamanan siber, antara lain melalui pelaksanaan *business impact analysis* secara berkala, sehingga kelangsungan usaha Bank dapat dipertahankan termasuk dengan menyertakan prosedur ketahanan dan kelangsungan usaha atas serangan keamanan siber dalam rencana pemulihan bencana (*disaster recovery plan*) dan rencana kontinjensi (*contingency plan*) disusun dengan menggunakan standar dan pedoman internasional dan nasional sebagai *benchmark* dan konsisten dengan kerangka manajemen risiko Bank secara menyeluruh (OJK, 2021).

Secara spesifik dapat dilakukan sebagai berikut kepatuhan sumber daya manusia terhadap kebijakan manajemen risiko keamanan siber termasuk sanksi yang dikenakan apabila terjadi pelanggaran, keamanan informasi termasuk pengaturan mengenai otentikasi melalui satu ID yang unik dan tenggat waktu kadaluarsa hak akses akun pengguna, prosedur penambahan, perubahan, atau penghapusan hak akses dalam hal perpindahan karyawan dan prosedur pelaporan dari karyawan dan klien terkait manajemen data menggunakan berbagai teknik, seperti perlindungan, transfer, dan penghapusan data, pengendalian kriptografi, kepatuhan terhadap undang-undang hak kekayaan intelektual, dan verifikasi seluruh perangkat keras dan perangkat lunak yang dibeli dari luar Bank. Teknik-teknik ini termasuk, tetapi tidak terbatas pada, analisis statis dan dinamis untuk memastikan bahwa protokol pengkodean aman telah diterapkan dengan benar (OJK, 2021).

Untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi, bank menerapkan manajemen keamanan data dan informasi (baik digital maupun kertas) untuk memastikan bahwa data dan dokumen dikelola sesuai dengan strategi risiko organisasi. Manajemen keamanan data termasuk, tetapi tidak terbatas pada Perlindungan *data-at-rest, data-at-endpoint, dan data-in-transit* termasuk enkripsi data dan informasi saat disimpan dan dikirim; pengelolaan aset (data dan informasi) yang memadai (aset yang dipindahkan, didisposisikan, atau tidak digunakan) perlindungan ketersediaan data dan informasi, termasuk kepemilikan data, metadata periode retensi, dan penggunaan terutama untuk data sensitif, termasuk data stakeholder. Mekanisme pengecekan integritas untuk verifikasi perangkat lunak, perangkat keras, dan integritas data dan

informasi; pemisahan lingkungan pengembangan dan pengujian dari lingkungan produksi; penggunaan mekanisme pengecekan integritas data untuk verifikasi perangkat keras; proses *backup* data yang dilakukan sesuai dengan kebutuhan bisnis berdasarkan hasil analisis dampak bisnis; dan penyimpanan *data backup* yang dilindungi secara fisik dan non-fisik, dan dokumen (OJK, 2021).

Bank menerapkan sistem manajemen untuk melindungi akses dan pengguna dengan mempertimbangkan hal-hal berikut, menggunakan identifikasi dan autentikasi untuk mengelola akses terhadap seluruh sistem, aplikasi, dan *hardware*, mengelola akses pengguna, termasuk kekompleksan kata sandi, pembatasan percobaan dan penggunaan kembali kata sandi, dan permintaan kata sandi setelah perangkat tidak aktif untuk beberapa saat. menerapkan pengamanan endpoint, antara lain dengan menggunakan filter web URL, pengendalian perangkat, dan pengendalian aplikasi pada seluruh perangkat endpoint pengguna. Menggunakan reputasi IP untuk memastikan bahwa alamat IP yang diizinkan digunakan dalam proses transaksi, memastikan batasan akses pada database, seperti mengizinkan akses hanya untuk pengguna selain administrator database, menggunakan autentikasi multi-faktor (MFA) untuk mendapatkan akses ke data sensitif atau ke seluruh jaringan jika diperlukan, menonaktifkan komunikasi antar workstation untuk mencegah serangan siber, dan menonaktifkan komunikasi antar pengguna pada klien nirkabel dalam tugas (OJK, 2021). Penelitian oleh (Akinbowale et al., 2024a) memaparkan bahwa kombinasi teknologi anti-penipuan internal dan eksternal, seperti perangkat lunak penyaringan, firewall, enkripsi, audit berkelanjutan, pengambilan sampel penemuan, perlindungan virus, rasio keuangan, analisis digital, dan penggalian data, dapat membantu mengurangi penipuan siber.

Kesimpulan

Perkembangan perbankan digital telah menuntut konsumen dan nasabah mengharapkan bahwa layanan perbankan harus aman dan mudah diakses, perkembangan dan inovasi di bidang keuangan dipengaruhi oleh peningkatan yang signifikan dalam jumlah pengguna internet setiap tahun. Aspek – aspek perkembangan perbankan digital di Indonesia terdapat bank terus mengembangkan layanan perbankan yang inovatif, seperti membuka rekening secara online, melakukan transaksi perbankan melalui aplikasi mobile, dan menyediakan layanan investasi dan pinjaman digital. Seiring dengan kemajuan teknologi, tuntutan untuk mengubah layanan keuangan ke dunia digital untuk memenuhi kebutuhan masyarakat semakin meningkat, terutama selama pandemi. Akibatnya, penyedia layanan keuangan, khususnya perbankan, harus berinovasi untuk memberikan layanan yang lebih baik dan memberikan nilai tambah kepada pelanggan. Seiring dengan kemajuan teknologi, perbankan digital menghadapi tantangan yang terus berkembang dalam hal keamanan.

Bank dapat menjadi sumber risiko siber seperti kurangnya pengujian pengamanan, kontrol, dan monitoring ancaman dan kerentanan, kelemahan sistem, serta tidak tersedianya anti malware/ anti-virus, dan sistem yang tidak update menjadi jalan bagi masuknya risiko siber kepada Bank. Faktor eksternal yang paling signifikan yang menyebabkan risiko siber bagi bank adalah kesadaran keamanan nasabah yang rendah dan peningkatan strategi dan kemampuan pelaku serangan siber. Dampak dari serangan risiko siber pada perkembangan perbankan digital di Indonesia yaitu kerugian yang dapat dihitung dan berdampak langsung pada bank disebut kerugian langsung. Kerugian tidak langsung adalah kerugian yang sulit dihitung secara kuantitatif, tetapi dapat mengurangi efisiensi operasional bank. Risiko Siber pada perkembangan perbankan digital di

Indonesia perlu diatasi dengan memuat bagaimana Bank menetapkan toleransi risiko keamanan siber dan tata cara Bank mengidentifikasi, mengurangi, dan mengelola risiko keamanan siber untuk mencapai keamanan siber. Diharapkan strategi ini dapat diterapkan secara baik oleh perbankan digital agar dapat meminimalisir risiko siber untuk kedepanya. Diharapkan dapat menjadi rujukan penelitian dalam melakukan analisis risiko siber terutama pada temuan empiris untuk kedepanya.

BIBLIOGRAFI

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024a). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, *31*(1), 201–225. https://doi.org/10.1108/JFC-02-2023-0025

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024b). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*, *31*(2), 287–301. https://doi.org/10.1108/JFC-10-2022-0260

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.

Aripin, N. T., Fatwa, N., Hannase, M., Pasca, P., Kajian, S., Tengah, T., & Islam, D. (2022). Layanan Digital Bank Syariah Sebagai Faktor Pendorong Indeks Literasi Dan Inklusi Keuangan Syariah. In *Jurnal Rumpun Ekonomi Syariah* (Vol. 5, Issue 1).

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. In *Journal of Financial Crime*. Emerald Publishing. https://doi.org/10.1108/JFC-10-2023-0263

Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*, *26*(6), 678–707. https://doi.org/10.1108/DPRG-02-2024-0029

Chhabra Roy, N., & Prabhakaran, S. (2023). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, *75*(2), 246–296. https://doi.org/10.1108/AJIM-11-2021-0339

Hill, -Napoleon. (2021). *Cetak Biru Transformasi Digital Perbankan*. Otoritas Jasa Keuangan. https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Cetak-Biru-Transformasi-Digital-Perbankan/Cetak%20biru%20transformasi%20digital%20perbankan%20(Short%20version).pdf

ISACA. (2022). *Cybersecurity and Technology Risk in Virtual Banking*. https://engage.isaca.org/

Mamun, S., & Ningsih, T. H. (2021). Implementasi Strategi Layanan Teknologi Digital Banking dan Service Quality dalam Perspektif Nasabah pada Perbankan Syariah (Study kasus pada Bank Syariah Mandiri KCP Tomang). *Jurnal Ekonomi Syariah Pelita Bangsa*, *6*(02), 223–233. https://doi.org/10.37366/jespb.v6i02.249

Muhammad, P., Penerbit, Z., Zaini, M., Saputra, N., Penerbit, Y., Lawang, K. A., & Susilo, A. (2023). *Metodologi Penelitian Kualitatif*. https://www.researchgate.net/publication/370561417

OJK. (2021). *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*.

Petani Masih Jauh Panggang Dari Api Hal, K. (2021). *Bangkitnya Era Bank Digital Di Indonesia : Prospek Dan Tantangan* (1). www.puskajianggaran.dpr.go.id
Sriekaningsih, A. (2020). *QRIS dan Era Baru Transaksi Pembayaran 4.0*. Penerbit Andi.
Wulandari, D. (2023). Pemasaran Produk Bank Syariah di Era Digital. *Jurnal Pendidikan Tambusai*, *7*(1), 3085-3092.

Copyright holder:
Ilham Zharfan Satrya (2024)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under:

