Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 1, Issue 5, 2023 pp. 154-160 http://urj.uin-malang.ac.id/index.php/mij/index

Enhancing *cybersecurity* in Bank Syariah Indonesia: Strategi menjaga data nasabah dan mencegah serangan *cyber*

M. Yusfil Anam
Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail : 200503110066@student.uin-malang.ac.id

Kata Kunci:
keamanan cyber; data nasabah; perlindungan data; strategi keamanan

Keywords:
cybersecurity; customer data; data protection; security strategies

A B S T R A K

Keamanan siber telah menjadi fokus utama dalam industri perbankan modern, terutama setelah serangan siber yang melibatkan Bank Syariah Indonesia (BSI) dan mengakibatkan kerugian besar bagi bank dan nasabahnya. Artikel ini menginvestigasi strategi yang dapat diterapkan oleh lembaga keuangan untuk meningkatkan sistem pertahanan mereka terhadap ancaman siber, dengan penekanan pada perlindungan data nasabah dan pencegahan serangan cyber. Melalui tinjauan literatur dan analisis mendalam, kami menyajikan berbagai strategi, termasuk penerapan teknologi keamanan informasi seperti Security Operation Center (SOC) dan enkripsi data sensitif, zero trust, GPN dan implementasi teknologi blockchain pada sistem IT perbankan. Kami juga mengulas peran yang dimainkan oleh Otoritas Jasa Keuangan (OJK) melalui regulasi dan pedoman mereka dalam mendukung ketahanan dan keamanan siber dalam sektor perbankan. Artikel ini memberikan wawasan yang mendalam tentang upaya-upaya yang diperlukan untuk memitigasi risiko keamanan siber di dalam dunia perbankan, dengan harapan dapat mendorong perbankan untuk mengadopsi strategi yang holistik dan proaktif dalam memitigasi risiko cyber dan melindungi data berharga nasabah.

A B S T R A C T

Cybersecurity has emerged as a paramount concern in the modern banking industry, particularly in the wake of the cyberattack involving Bank Syariah Indonesia (BSI) that led to significant losses for the bank and its customers. This article delves into strategies that financial institutions can adopt to bolster their defense systems against cyber threats, with a focus on safeguarding customer data and preempting cyber attacks. Through an in-depth review of literature and analysis, we present an array of strategies, including the implementation of information security technologies such as Security Operation Centers (SOCs) and sensitive data encryption, along with the adoption of a zero trust model, Global Private Network (GPN), and the integration of blockchain technology into banking IT systems. We also examine the role played by the Financial Services Authority (OJK) through its regulations and guidelines in reinforcing resilience and cybersecurity within the banking sector. This article offers profound insights into the necessary endeavors to mitigate cybersecurity risks within the banking realm, with the aspiration of incentivizing banks to embrace holistic and proactive strategies in navigating cyber risks and safeguarding invaluable customer data.

Pendahuluan

Pada zaman ini, permintaan akan layanan teknologi informasi dan komunikasi berkembang begitu cepat untuk menunjang berbagai kebutuhan layanan, terutama dibidang jasa seperti perbankan, e-commerce dan teknologi kerja hingga game dan

streaming online. Teknologi komunikasi informasi ini sangat berperan penting dalam menjaga keberlangsungan suatu bisnis, pekerjaan, pendidikan, layanan dan komunikasi (Minai et al., 2021).

Menurut badan pusat statistik indonesia, selama kurun waktu lima tahun kebelakang dari 2017 hingga tahun 2021, perkembangan teknologi informasi komunikasi di indoensia mengalami tren positif (Mukrimaa et al., 2016). Perkembangan teknologi ini tidak dapat dihentikan karena linear dengan keinginan manusia akan kenyamanan, kemudahan dan fleksibilitas dalam setiap aspek aktifitasnya (Kholis, 2020). Dalam industri jasa perbankan, mengikuti genangan kemajuan zaman dan teknologi digital merupakan suatu kemustahilan untuk tidak dilakukan. Selain itu, teknologi sistem informasi pada perbankan sangat lumrah dimanfaatkan oleh bank sebagai pengolah data keuangan serta menerapkan layanan pada perbankan aecara digital dengan menggunakan sarana kompterisasi, telekomunikasi serta berbagai sarana elektronik lainnya (Nurhasanah & Nasution, 2022). Hal ini disebabkan beberapa ekosistem bisnis yang terus berubah seiring kemajuan teknologi dan tuntutan nasabah akan kemudahan, keamanan, efesien serta fleksibilitas dalam layanan jasa perbankan digital (Laucereno, 2022). Penelitian lain juga mengungkapkan bahwa penggunaan teknologi informasi dalam layanan perbankan digital dapat meningkatkan loyalitas nasabah kepada bank (Nguyen, 2020).

Layanan perbankan digital berbasis teknologi informasi memang membutuhkan dana yang tidak sedikit. Hal ini jelas disebabkan oleh beberapa faktor seperti kondisi infrastruktur yang kurang mencukupi dan luas geografis indonesia yang unik. Akan tetapi, perbankan dan lembaga keuangan baik konvensional maupun syariah sangat dipengaruhi oleh perkembangan produk-produk teknologi informasi, sehingga tidak dapat lagi berfungsi tanpaadanyav (Dz., 2018). Maka dari itu, penting untuk mengoptimalkan sebuah inovasi untuk menyeselasiakan pusat layanan dengan menempatkan teknologi informasi komunikasi melalui digitalisasi layanan sehingga hubungan antar bank dengan nasabah menjadi lebih erat, efesien, cepat, mudah dan fleksibel.

Pemanfaatan TI di industri perbankan menghadapi banyak tantangan, salah satu diantaranya adalah peretasan sistem informasi disertai pencurian data nasabah perbankan oleh hacker. Di indonesia, sektor paling rentan terhadap serangan siber adalah sektor keuangan yang menduduki peringkat kedua dari banyaknya kasus serangan siber, sebagaimana yang dilaporkan oleh OJK pada mei 2022 (Tarigan & Paulus, 2019).

Serangan siber terhadap Bank Syari'ah Indeonesia (BSI) pada 8 bulan Mei 2023 menunjukkan risiko keamanan siber yang nyata dalam industri jasa perbankan. Serangan ini diduga kuat akibat adanya ransomware. Keamanan data perbankan nasabah menjadi sebuah isu yang sangat penting karena data nasabah perbankan biasanya berisi informasi personal dan bersifat sensitif yang dapat disalahgunakan untuk tindak kejahatan seperti pencurian identitas atau penipuan, meskipun perlindungan hukum terhadap nasabah atas risiko dari layanan perbankan digital telah diatur oleh Pearturan OJK No.12/POJK.03/2018 yang merupakan perlindungan preventif terkait nasabah.

Bank syariah menghadapi risiko yang begitu kompleks, entah itu finansial ataupun non finansial termasuk juga risiko yang berkaitan dengan pemanfaatan penggunaan layanan teknologi modern. Risiko ini sangat umum di kalangan pelanggan milenial dan sangat rentan terhadap ancaman kejahatan siber, maka perlu adanya langkah-langkah perlindungan. Sebuah penelitian menunjukkan bahwa adanya kekurangan keahlian dalam manajemen risiko dan mitigasi di bank syariah dibandingkan konvensional (Eni, 1967). Hal ini menunujukkan bahwa bank syariah perlu meningkatkan manajemen risiko untuk memberikan informasi kepada regulator mengenai risiko dalam mencegah bank dari berbagai resiko yang cenderung tidak dapat dikendalikan serta mitigasi risiko untuk melindungi diri serta data nasabah mereka dari risiko keamanan siber dan lainnya (Syadali et al., 2023).

Sebagai lembaga bergerak dibidang jasa yang menangani uang dan transaksi masyarakat, perbankan harus memberikan jaminan keamanan yang maksimal terhadap data keuangan nasabah. Kemanan siber sangat penting khususnya bagi industri keuagan karena berkaitan dengan data dan informasi pribadi nasabah yang dapat merusak reputasi bank dan kepercayaan nasabah. Selain itu, penggunaan teknologi semakin banyak dibutuhkan oleh perusahaan, termasuk perbankan. Namun penggunaan teknologi juga dapat membawa risiko keamaan yang tinggi, seperti serangan siber (Fasounaki et al., 2021). Maka dari itu, semua bank khusunya BSI harus mampu mencegah risiko kebocoran data nasabah dengan mitigasi risiko yang tepat untuk pencegahan serangan siber yang probalitas terjadi.

Metode penulisan artikel ini akan mencakup pendekatan deskriptif dan analisis untuk menjelaskan secara menyeluruh tentang masalah keamanan siber dalam perbankan dan bagaimana meningkatkan sistem pertahanannya. Artikel ini juga akan didukung dengan data dan referensi yang kuat untuk mendukung argumen dan kesimpulan yang diajukan.

Pembahasan

Perbankan modern saat ini khusunya BSI, bergantung pada teknologi dan platfrom digital untuk menjalankan sistem operasional mereka dan bersaing sesama lain (Kartika & Segaf, 2022; Kornelis, 2022). Namun ketergantungan ini juga menghadirkan kerentanan terhadap serangan siber yang dapat mencuri data sensitif nasabah, meretas sistem pencatatan perbankan bahkan sampai melmupuhkan seluruh sistem operasi perbankan (Ngamal & Maximus Ali Perajaka, 2021).

Kabar menyebutkan bahwa informasi internal yang dimiliki oleh PT Bank Syariah Indonesia Tbk (BSI) diduga telah terungkap di lapisan tersembunyi internet, yang dikenal sebagai dark web, akibat dari serangan Ransomware. Para pakar dalam bidang keamanan siber menganggap bahwa ketika data tersebut bocor secara meluas, biasanya akan diikuti oleh upaya phishing yang dapat menipu banyak pihak untuk keuntungan pribadi. Ransomeware ini sangat bahaya karena merupakan sejenis Software yang dapat mengambil alih kemudi komputer dan mencegah user untuk mengkases data biasanya, pembuat virus ini menunut uang tebusan agar sistem

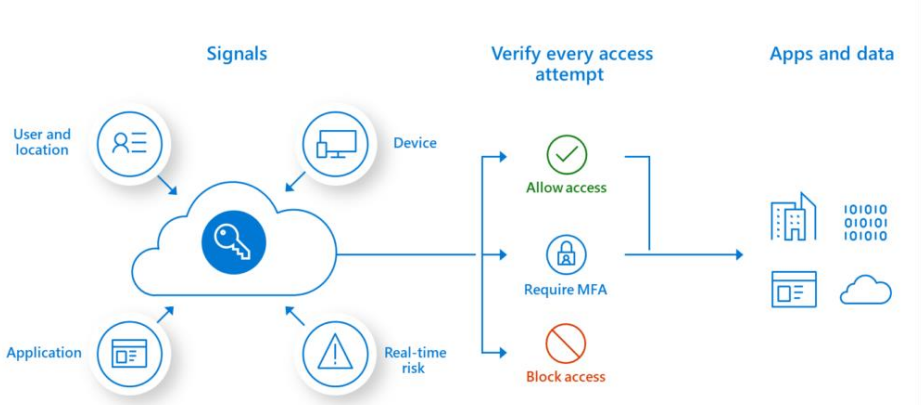
kembali. Sementara itu, phishing merujuk pada usaha memperoleh data pribadi seseorang dengan cara meniru atau menyamar.

Sebuah kelompok peretas internasional yang menggunakan Ransomware, yakni LockBit 3.0, mengumumkan bahwa mereka berhasil mengakses data internal PT Bank Syariah Indonesia Tbk (BSI) dan menyebarkan informasinya di dark web. Tindakan ini diambil setelah terduga bahwa persatuan tiga bank syariah yang terlibat tidak memenuhi permintaan LockBit 3.0 untuk membayar tebusan sebesar US $20 juta atau sekitar Rp295,6 miliar. Informasi ini diperoleh melalui unggahan gambar oleh akun Twitter dari entitas keamanan teknologi, yaitu Fusion Intelligence Center dengan nama pengguna DarkTracer. Dalam unggahannya, akun tersebut membagikan screenshot yang menunjukkan informasi yang diperkirakan berasal dari data BSI yang telah bocor.

Tren akan teknologi, perbankan modern mengadopsi berbagai teknologi keamanan informasi untuk melindungi data nsabah mereka, berikut beberapa teknologi keamanan informasi yang digunakan oleh perbankan modern untuk menjaga data:

1. Zero Trust Model: pendekatan ini mengasumsikan bahwa setiap akses ke jaringan atau sistem harus diverifikasi terlebih dahulu, meskpiun jika akses terebut berasal dari jaringan internal. Model ini sepenuhnya didukung oleh microsoft 365 untuk memberikan keamanan untuk para penggunanya yang salah satunya adalah bank.

Gambar 1.1 Skema perlindungan data



Dalam Flowchart gambar diatas, dapat diketahui bagaimana enkripsi yang digunakan oleh perbankan dalam mengakses sebuah data yang terhubung dalam software Microsoft, dimana semua akses baik internal harus melalui verifikasi terlebih dahulu untuk melindungi keamanan data dalam komputer.

2. Enkripsi data, teknologi yang mengubah data menjadi kode rahasia sehingga hanya orang yang memiliki kunci enkripsi yang dapat membaca data tersebut. Karena teknik enkripsi ini bisa mengacak pesan sehingga tidak dapat diketahui dan membentuk bidang keilmuan yang di juluki Kriptografi yang hanya bisa diakses oleh orang yang berwenang saja. Jadi bisa dikatakan teknik enkripsi menjadi lebih canggih, sebab telah menginputkan elemen matematika yang membuatnya cenderung sulit untuk memecahkan kode informasi (Nurcahya, 2022).
3. Identifikasi Biometrik, teknologi menggunakan ciri-ciri fisik unik, seperti sidik jari atau wajah untuk mengidentifikasi nasabah.

Dalam industri perbankan, keamanan informasi sangat penting untuk melindungi segenap data nasabah yang bersifat rahasia. Beberapa teknologi keamanan informasi yang umum digunakan oleh bank modern termasuk user identification, user authentication dan user authorization. Selain itu, beberapa ancaman yang mungkin terjadi pada sistem informasi termasuk hacking, intrupsion, denial of services dll. Berikut ini adalah beberapa alternatif metode yang efektif dalam meningkatkan sistem keamanan perbankan dan mencegah terjadinya serangan siber:

a. Implementasi sistem keamanan informasi, untuk menjaga keamanan sistem informasi menjadi suatu hal yang tak dapat diabaikan, terutama dalam sektor layanan perbankan yang semakin mengandalkan transaksi daring seperti layanan internet banking. Upaya yang dilakukan oleh bank dalam mengamankan sistem informasi mereka mencakup penerapan teknik-teknik mutakhir seperti penggunaan firewall untuk filtrasi data, penerapan enkripsi guna melindungi integritas informasi, dan penggunaan metode otentikasi multi-faktor agar sistem informasi tetap aman dari ancaman yang mungkin timbul.
b. Pengenalan Gerbang Pembayaran Nasional (GPN) merupakaan langkah yang diinisiasi oleh Bank Indonesia guna mendorong pertumbuhan transaksi nontunai di seluruh penjuru Indonesia. Melalui GPN, tercipta sebuah kerangka yang menghubungkan beragam jalur pembayaran, memungkinkan penggunaan beragam alat pembayaran dari berbagai bank dalam kanal yang sama. Implementasi GPN membawa berbagai keuntungan, termasuk keamanan sebuah transaksi, kemampuan bank dalam meningkatkan infrastruktur pembayaran mereka serta memberikan opsi pembayaran yang lebih efisien dan praktis bagi nasabah yang di layani (Kusumastuti & Tinangon, 2019).
c. Implementasi teknologi blockchain pada sistem IT perbankan dapat memperkuat keamanan dan efisiensi layanan perbankan. Berikut adalah beberapa manfaat dari implementasi teknologi blockchain pada sistem IT perbankan. Dalam penelitian yang dilakukan oleh Elan maulani Di ranah perbankan, pemanfaatan teknologi blockchain merupakaan cara yang efektif untuk menegakkan keutuhan data transaksi serta memastikan bahwa setiap transaksi yang terekam telah melalui proses validasi yang sah. Di sektor perdagangan, potensi teknologi blockchain sangat berarti dalam memastikan bahwa produk yang diperdagangkan memang berkualitas asli dan memiliki asal-usul yang dapat diverifikasi dengan jelas (Elan Maulani et al., 2023). Menigkatkan efisiensi operasional, Penerapan teknologi blockchain dalam infrastruktur IT perbankan memiliki potensi untuk mengurangi biaya yang terkait dengan setiap transaksi, sekaligus mempercepat kelancaran prosesnya. Kelebihan lainnya adalah, transaksi dapat terealisasikan tanpa memerlukan perantara seperti bank atau institusi keuangan lainnya. Menangani masalah double spending, Kemampuan teknologi blockchain dalam mengatasi double spending, yakni situasi di mana uang yang sama digunakan untuk transaksi berbeda, terlihat jelas. Informasi yang dimasukkan ke dalam rantai blok blockchain akan dijalankan dan diperiksa oleh jaringan blockchain itu sendiri, memastikan bahwa tidak akan ada transaksi yang diulang tanpa alasan yang sah.

Kesimpulan dan Saran

Ketika beroperasi di era digital yang kompleks ini, bank harus memprioritaskan keamanan siber sebagai bagian integral dari strategi bisnis mereka. Serangan siber dapat menyebabkan kerugian finansial yang besar, merusak reputasi, dan mengganggu kepercayaan nasabah. Dengan menerapkan strategi dan teknologi keamanan yang tepat, bank dapat mengurangi risiko keamanan siber dan melindungi data nasabah dengan lebih efektif. Canggihnya teknologi untuk mencegah serangan siber di perbakan, tidak bisa menjamin 100% terjaga. Karena semakin canggih sebuah teknologi, maka akan semakin canggih pula kejahatan-kejahatan di dunia maya. Keamanan siber merupakan hal yang krusial dalam dunia perbankan, mengingat semakin meningkatnya serangan siber yang mengancam data nasabah dan kestabilan institusi perbankan. Dalam rangka meningkatkan keamanan siber, bank perlu menerapkan strategi yang efektif dan berkelanjutan. Tak lupa juga regulasi dan pedoman dari OJK juga berperan penting dalam membantu bank menghadapi risiko keamanan siber dengan memberikan arahan dan standar yang jelas. Dengan mengimplementasikan strategi keamanan yang komprehensif dan berkelanjutan, bank dapat memastikan bahwa data nasabah tetap aman dan melindungi diri mereka dari potensi serangan siber di masa depan.

Daftar Pustaka

Dz., A. S. (2018). Inklusi Keuangan Perbankan Syariah Berbasis Digital-Banking: Optimalisasi dan Tantangan. *Al-Amwal : Jurnal Ekonomi Dan Perbankan Syari'ah*, *10*(1), 63. https://doi.org/10.24235/amwal.v10i1.2813

Elan Maulani, I., Herdianto, T., Febri Syawaludin, D., & Oga Laksana, M. (2023). Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi. *Jurnal Sosial Teknologi*, *3*(2), 99–102. https://doi.org/10.59188/jurnalsostech.v3i2.634

Eni. (1967). Manajemen Mitigasi Risiko Pada Bank Syariah. *Angewandte Chemie International Edition, 6(11), 951–952.*, *Mi*, 5–24.

Fasounaki, M., Yüce, E. B., Öncül, S., & Ince, G. (2021). CNN-based Text-independent Automatic Speaker Identification Using Short Utterances. *Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021*, *01*, 413–418. https://doi.org/10.1109/UBMK52708.2021.9559031

Kartika, G., & Segaf, S. (2022). Kombinasi Peran Model TAM dan CARTER Terhadap Optimalisasi Kepuasan Nasabah Mobile Syariah Banking di Masa Pandemi Covid-19. *Jurnal Manajerial*, *9*(02), 152–167.

Kholis, N. (2020). Perbankan Dalam Era Baru Digital. *Economicus*, *12*(1), 80–88. https://doi.org/10.47860/economicus.v12i1.149

Kornelis, Y. (2022). Digital Banking Consumer Protection: Developments & Challenges. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 378–394. https://doi.org/10.23887/jkh.v8i1.44477

Kusumastuti, A. D., & Tinangon, J. R. (2019). Penerapan Sistem Gpn (Gerbang Pembayaran Nasional) Dalam Menunjang Transaksi Daring. *Jurnal Bisnis Dan Manajemen*, *6*(1), 56–64. https://doi.org/10.26905/jbm.v6i1.3035

Laucereno, S. F. (2022). *Bank Jangan Ketinggalan Zaman, Layanan Harus Serba Digital*. DetikFinance. https://finance.detik.com/moneter/d-6407809/bank-jangan-ketinggalan-zaman-layanan-harus-serba-digital

Minai, M. S., Raza, S., & Segaf, S. (2021). Post COVID-19: Strategic digital entrepreneurship in Malaysia. In *Modeling economic growth in contemporary Malaysia* (pp. 71–79). Emerald Publishing Limited.

Mukrimaa, S. S., Nurdyansyah, Fahyuni, E. F., YULIA CITRA, A., Schulz, N. D., د, غسان., Taniredja, T., Faridli, E. Miftah., & Harmianto, S. (2016). Indeks Pembangunan Teknologi Informasi dan komunikasi 2021. In *Jurnal Penelitian Pendidikan Guru Sekolah Dasar* (Vol. 6, Issue August).

Ngamal, Y., & Maximus Ali Perajaka. (2021). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74. https://doi.org/10.33541/mr.v2iiv.4099

Nguyen, O. T. (2020). Faktor-faktor yang Mempengaruhi Niat Menggunakan Perbankan Digital di Vietnam. *Journal of Asian Finance, Economics and Business*, *7*(3), 303–310.

Nurcahya, S. D. (2022). *Sentosa Bank Customer Encrypted Data Information System Using Micro SD*. *6*(2), 528–536. https://doi.org/10.52362/jisicom.v6i2.952

Nurhasanah, U., & Nasution, M. I. P. (2022). Pengaruh Penggunaan Sistem Informasi terhadap Layanan Produk Bank Konvensional dan Bank Syariah. *Lensa Ilmiah: Jurnal Manajemen Dan Sumberdaya*, *1*(3), 176–181. https://doi.org/10.54371/jms.v1i3.211

Syadali, M. R., Segaf, S., & ... (2023). Risk management strategy for the problem of borrowing money for Islamic commercial banks. *Enrichment: Journal …* , *13*(2).

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 294–307. https://doi.org/10.14710/jphi.v1i3.294-307