Jurnal Ilmiah Wahana Pendidikan, June 2025, 11(6.D), 34-39
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/10707
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Menanggulangi Ancaman Keamanan Siber Di Sektor Perbankan : Upaya Melindungi Data Nasabah Di Zaman Digital

Aqilah Belva Nathania, Muhammad Adzkiya Azam, Renita Rachel Elizabeth Voll

Universitas Negeri Semarang

Received: 20 Mei 2025
Revised: 27 Mei 2025
Accepted: 01 Juni 2025

Abstrak

Perkembangan teknologi digital telah membawa perubahan signifikan dalam sektor perbankan, namun juga meningkatkan kerentanannya terhadap ancaman keamanan siber. Ancaman seperti peretasan, pencurian data, dan penipuan digital menjadi masalah utama yang mengancam integrasi sistem perbankan dan melibatkan data pribadi nasabah. Artikel ini membahas tantangan yang dihadapi sektor perbankan dalam menjaga keamanan siber, serta upaya-upaya yang dapat dilakukan untuk melibatkan data pribadi nasabah. Artikel ini membahas tantangan yang dihadapi sektor perbankan dalam menjaga keamanan siber, serta upaya-upaya yang dapat dilakukan untuk melindungi data nasabah di era digital. Dengan meningkatkan ancaman terhadap sistem digital, sektor perbankan harus mengadopsi pendekatan yang lebih proaktif dan berkelanjutan dalam memperkuat pertahanan terhadap serangan siber, guna memastikan perlindungan maksimal terhadap data nasabah.

Kata Kunci: *Keamanan siber, Sektor perbankan, Perlindungan data nasabah.*

(*) Corresponding Author: aqilahbelvaa@students.unnes.ac.id, rachelizaav@students.unnes.ac.id, adzkiyaaaa@students.unnes.ac.id

How to Cite: Nathania, A., Azam, M., & Voll, R. (2025). Menanggulangi Ancaman Keamanan Siber Di Sektor Perbankan : Upaya Melindungi Data Nasabah Di Zaman Digital. *Jurnal Ilmiah Wahana Pendidikan*, *11*(6.D), 34-39. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/10707

PENDAHULUAN

Perkembangan teknologi digital telah mengubah wajah sektor perbankan secara signifikan. Di era dimana hampir semua transaksi dilakukan secara online, bank kini dituntut untuk beradaptasi dengan cepat terhadap perubahan ini. Transformasi digital memungkinkan nasabah untuk mengakses layanan perbankan dengan lebih mudah dan cepat, mulai dari pembukaan rekening hingga transaksi keuangan yang kompleks, semuanya dapat dilakukan hanya dengan beberapa klik. Namun, kemudahan ini juga datang dengan risiko yang tidak bisa diabaikan. Transformasi digital yang terjadi dalam sektor perbankan memang membawa banyak kemudahan, namun dibalik itu, muncul berbagai celah yang dapat dimanfaatkan oleh ancaman siber. Ancaman seperti peretasan, pencurian data, dan penipuan online kini menjadi tantangan serius yang harus dihadapi oleh lembaga keuangan. Ketergantungan yang semakin tinggi pada sistem digital membuat perlindungan data nasabah menjadi prioritas utama bagi bank. Namun, masalahnya tidak hanya berasal dari luar; ancaman juga bisa muncul dari dalam, seperti tindakan karyawan yang menyalahgunakan akses mereka.

Hal ini menegaskan bahwa keamanan siber perlu menjadi perhatian menyeluruh yang melibatkan semua pihak—dari manajemen bank hingga nasabah itu sendiri. Edukasi tentang keamanan informasi sangat penting agar nasabah dapat melindungi data pribadi mereka dari berbagai metode penipuan yang terus berkembang. Dengan meningkatnya kompleksitas ancaman ini, lembaga perbankan harus proaktif dalam menerapkan langkah-langkah keamanan sebagai tindak preventif. Dengan kata lain, kerjasama antara bank dan nasabah sangat penting untuk menciptakan lingkungan perbankan yang aman di era digital saat ini.

Sukses dalam menghadapi ancaman siber tidak hanya bergantung pada teknologi yang canggih, tetapi juga pada kesadaran dan keterlibatan aktif dari semua pihak yang terlibat. Dalam menghadapi ini, sektor perbankan perlu terus beradaptasi dan memperbarui strategi keamanannya agar bisa lebih efektif dalam menghadapi berbagai tantangan yang ada.

METODE PENELITIAN

Penelitian ini menggunakan tipe penelitian sosio-yuridis. Dimana penelitian ini bersifat eksploratif. Penelitian dilakukan dengan menghubungkan dan mencari hipotesis dari fenomena-fenomena tertentu. Sumber data dari penelitian ini adalah data sekunder yang diperoleh dari buku-buku, tulisan dan kajian yang terdahulu dan berkaitan dengan penelitian ini. Teknik penelitian ini adalah melalui metode Kepustakaan (Library Methode). Semua bahan hukum yang terkumpul dianalisis secara kualitatif, lalu penulis mendeskripsikan untuk menjawab permasalahan dalam penelitian ini.

HASIL & PEMBAHASAN

Bentuk Ancaman Keamanan Siber Yang Dihadapi Sektor Perbankan Dalam Era Digital

Sektor perbankan di era digital menghadapi berbagai bentuk ancaman keamanan siber yang dapat mengancam integritas sistem, data nasabah, dan stabilitas operasional. Peretasan atau hacking dimana penyerang mencoba untuk mengakses sistem perbankan secara ilegal dengan tujuan mencuri data atau merusak sistem. Peretasan ini dapat mengakibatkan pencurian informasi sensitif seperti data nasabah, rincian transaksi, dan informasi akun, yang dapat dimanfaatkan untuk penipuan atau kejahatan.

Terdapat juga metode penipuan yang dikenal dengan sebutan phising, dimana pelaku mengirimkan email atau pesan yang tampak sah, tetapi berisi link atau lampiran berbahaya untuk mencuri informasi pribadi. Nasabah yang tertipu dapat memberikan informasi akun mereka, seperti username, password, atau data kartu kredit, yang kemudian dapat digunakan untuk akses ilegal. Terdapat juga malware dan ransomware dimana perangkat lunak berbahaya yang dirancang untuk merusak sistem atau mencuri data. Ransomware adalah jenis malware yang mengenkripsi data dan meminta tebusan untuk mendekripsinya, dimana hal ini berdampak bank dan nasabah dapat kehilangan data penting, dan bank bisa terpaksa membayar tebusan atau mengalami kerusakan reputasi dan operasional yang besar.

Terdapat juga Serangan DDoS (Distributed Denial of Service) yaitu serangan yang membanjiri server bank dengan lalu lintas data berlebihan untuk membuatnya tidak dapat diakses, mengganggu operasional bank dan pelayanan kepada nasabah. Ancaman lainnya Man-in-the-Middle (MITM) adalah jenis serangan siber di mana penyerang menyusup di antara komunikasi nasabah dan bank untuk mencuri informasi atau manipulasi transaksi. Penyerang dapat mengubah rincian transaksi atau mengakses informasi pribadi yang dikirimkan antara kedua belah pihak. Ancaman MITM sering terjadi ketika nasabah mengakses layanan perbankan melalui jaringan Wi-Fi publik yang tidak aman, yang memberikan celah bagi penyerang untuk melakukan intersepsi data.

Selain itu terdapat juga Skimming dan card cloning yang juga merupakan ancaman besar bagi nasabah dan bank. Dengan perangkat skimmer yang dipasang pada mesin ATM atau terminal pembayaran, penjahat siber dapat menyalin data kartu kredit atau debit nasabah secara ilegal. Data yang dicuri ini kemudian digunakan untuk melakukan transaksi ilegal atau mengakses dana nasabah. Fenomena ini menunjukkan bagaimana teknologi yang tidak aman dapat dimanfaatkan untuk menembus sistem perbankan.

Selain ancaman melalui eksternal, sektor perbankan juga harus mewaspadai ancaman dari dalam (insider threats). Ancaman ini berasal dari pegawai bank yang memiliki akses ke sistem dan data sensitif nasabah. Meskipun sangat sulit untuk dideteksi, ancaman dari dalam dapat terjadi jika pegawai tersebut menyalahgunakan akses mereka untuk mencuri data atau merusak sistem secara sengaja. Keamanan internal yang ketat dan pemantauan terus-menerus terhadap aktivitas pegawai menjadi penting untuk mencegah jenis ancaman ini.

Kebocoran data (data breach) adalah ancaman serius lainnya, yang terjadi ketika informasi pribadi nasabah atau data keuangan bank bocor dan jatuh ke tangan yang salah. Kebocoran data ini bisa terjadi karena kelalaian pegawai, serangan peretasan, atau kesalahan dalam pengelolaan data. Jika data nasabah bocor, bank tidak hanya berisiko kehilangan kepercayaan nasabah, tetapi juga dapat menghadapi tuntutan hukum dan denda besar dari regulator.

Dalam menghadapi ancaman-ancaman ini, sektor perbankan harus mengimplementasikan berbagai langkah keamanan yang komprehensif. Salah satunya adalah dengan menggunakan enkripsi untuk melindungi data transaksi dan informasi pribadi nasabah. Selain itu, penerapan otentikasi dua faktor (2FA) akan menambah lapisan keamanan dalam proses login dan transaksi online. Kecerdasan buatan (AI) dan machine learning juga dapat digunakan untuk mendeteksi pola serangan siber dan merespons ancaman secara real-time. Bank juga perlu bekerja sama dengan regulator dan pihak ketiga yang memiliki standar keamanan tinggi untuk menjaga integritas sistem mereka. Tidak hanya itu, edukasi kepada nasabah mengenai pentingnya menjaga kerahasiaan informasi pribadi dan menghindari ancaman siber juga menjadi langkah penting dalam mitigasi risiko.

Sehingga sektor perbankan harus terus beradaptasi dengan ancaman-ancaman baru di dunia siber. Keamanan siber bukan hanya tanggung jawab teknis dari lembaga perbankan, tetapi juga melibatkan kesadaran dan partisipasi aktif nasabah serta pihak terkait lainnya. Hanya dengan pendekatan yang holistik dan proaktif, bank dapat melindungi data nasabah dan menjaga keberlanjutan operasional mereka di era digital yang penuh tantangan ini.

Langkah-Langkah Yang Telah Diambil Oleh Lembaga Perbankan Dan Regulasi Yang Ada Indonesia Untuk Melindungi Data Nasabah Dalam Ancaman Keamanan Siber

Lembaga perbankan di Indonesia telah mengambil berbagai langkah untuk melindungi data nasabah dari ancaman keamanan siber, mengingat meningkatnya risiko yang dihadapi di era digital ini. Pertama-tama, mereka menerapkan teknologi enkripsi untuk melindungi data sensitif saat ditransfer, sehingga informasi pribadi nasabah tetap aman dari tangan-tangan yang tidak bertanggung jawab. Selain itu, banyak bank yang kini mengadopsi otentikasi dua faktor (2FA) sebagai langkah tambahan untuk memastikan bahwa hanya nasabah yang berwenang yang dapat mengakses akun mereka. Langkah ini terbukti efektif dalam mengurangi risiko pencurian identitas dan akses ilegal. Tidak hanya itu, lembaga perbankan juga aktif dalam melakukan edukasi kepada nasabah tentang pentingnya menjaga kerahasiaan informasi pribadi dan mengenali potensi ancaman seperti phishing. Melalui kampanye edukasi ini, nasabah diharapkan lebih waspada terhadap berbagai metode penipuan yang terus berkembang. Di samping itu, bank juga bekerja sama dengan regulator seperti OJK untuk memastikan bahwa mereka mematuhi standar keamanan yang ketat dan melakukan audit secara berkala terhadap sistem keamanan mereka. Banyak bank kini menggunakan kecerdasan buatan (AI) untuk mendeteksi pola serangan siber dan merespons ancaman dengan cepat.

Dampak Dari Ancaman Keamanan Siber Terhadap Data Nasabah Dan Reputasi Bank

Dalam perkembangan teknologi atau era digitalisasi banyak sekali ancaman yang mengancam keamanan siber, keamanan siber merupakan salah satu isu yang semakin mendesak di era digital ini, khususnya bagi industri perbankan yang mengelola data pribadi

dan finansial nasabah. Dalam beberapa tahun terakhir, serangan siber terhadap lembaga keuangan telah meningkat secara signifikan, dengan dampak yang bisa sangat merugikan, baik bagi nasabah maupun bagi bank itu sendiri. Serangan siber akhir - akhir ini yang sering mengancam data nasabah adalah dengan menggunakan metode phising, phishing sendiri merupakan metode untuk memperoleh informasi pribadi seseorang dengan menggunakan teknik penipuan. Data yang sering menjadi target phishing meliputi informasi pribadi (seperti nama, usia, alamat), data akun (seperti username dan password), serta data finansial (misalnya informasi kartu kredit atau nomor rekening). Menurut Kementrian Keuangan sendiri terdapat beberapa jenis dari phising[1]:

1. Email Phishing

Seperti namanya, email phishing memanfaatkan media email untuk menipu calon korban. Tindakan phishing melalui email ini cukup sering terjadi, dengan data menunjukkan sekitar 3,4 miliar email palsu dikirim setiap hari. Angka ini menunjukkan seberapa besar potensi korban yang dapat terjebak.

2. Spear Phishing

Spear phishing merupakan jenis phishing yang lebih terarah. Berbeda dengan email phishing yang mengirimkan email ke banyak orang secara acak, spear phishing menargetkan individu tertentu. Teknik ini biasanya dilakukan setelah memperoleh informasi dasar tentang korban, seperti nama dan alamat.

3. Whaling

Whaling adalah bentuk phishing yang menyasar individu dengan posisi tinggi dalam suatu organisasi, seperti pemilik bisnis, direktur perusahaan, atau manajer HR. Jika aksi whaling ini berhasil, para pelaku dapat memperoleh keuntungan besar dari akses yang didapatkan.

4. Web Phishing

Web phishing melibatkan pembuatan situs web palsu yang dirancang untuk menipu calon korban. Website tersebut dibuat agar mirip dengan situs resmi dan menggunakan nama domain yang hampir serupa, sebuah teknik yang dikenal dengan istilah domain spoofing.

Dari beberapa ancaman yang telah disebutkan diatas terdapat banyak sekali dampak bagi dunia perbankan di Indonesia, termasuk dalam sektor data nasabah dan reputasi bank, mulai dari metode email phishing yang bisa mengambil dari data kartu kredit kartu pengguna mulai dari pin, data diri hingga pada akhirnya bisa menguras habis dana yang dimiliki oleh si pemilik kartu, selanjutnya dampak bagi bank sendiri dapat mengurangi reputasi dari bank tersebut dikarenakan jika terdapat nasabah yang terkena email phishing maka akan semakin sedikit orang yang akan membuka rekening di bank tersebut.

Serangan siber tidak hanya membahayakan nasabah tetapi juga dapat mengakibatkan kerugian finansial yang signifikan bagi bank. Sebagai contoh, jika terjadi serangan ransomware di mana peretas mengunci data penting dan sistem bank, bank mungkin dipaksa membayar sejumlah uang sebagai tebusan untuk mendapatkan kembali data yang terkontaminasi atau terkunci. Pembayaran tebusan ini, yang seringkali sangat tinggi, hanyalah satu bagian dari kerugian yang dialami bank. Bank juga harus mengeluarkan biaya besar untuk memperbaiki sistem yang rusak, memulihkan data yang hilang, dan melakukan audit dan penilaian keamanan untuk mencegah serangan serupa.

Biaya pemulihan mungkin termasuk biaya penggantian perangkat keras dan perangkat lunak yang rusak, serta biaya menyewa spesialis forensik siber untuk menyelidiki. dan menemukan sumber serangan, serta biaya untuk memperbarui sistem keamanan untuk

[1] Fanasafa I, *Waspada! Kejahatan Phising Mengintai Anda* (Jum'at, 25 Maret 2022), https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html

menutup celah yang digunakan peretas. Bank harus melakukan tindakan tambahan untuk memperbaiki reputasi yang rusak yang mereka miliki di mata pelanggan dan masyarakat umum, karena hal ini dapat mempengaruhi kepercayaan dan loyalitas pelanggan, bahkan setelah serangan berhasil diatasi.

Selain itu, biaya hukum dan peraturan dapat menyebabkan kerugian keuangan. Bank dapat dikenakan sanksi atau denda yang cukup besar jika regulator atau pengawas menemukan bahwa mereka tidak mematuhi peraturan keamanan atau tidak mengambil tindakan yang cukup untuk melindungi data pelanggan. Pengenaan denda ini dapat merugikan posisi keuangan bank dan memperburuk reputasinya. Selain itu, bank mungkin menghadapi tuntutan hukum dari pelanggan atau pihak lain yang merasa dirugikan karena kebocoran data atau gangguan dalam layanan. Oleh karena itu, kerugian moneter yang ditimbulkan oleh serangan siber dapat mencakup konsekuensi jangka panjang terhadap stabilitas dan kelangsungan operasional bank, selain biaya langsung untuk memperbaiki kerusakan.

PENUTUP

Kesimpulan

Perkembangan teknologi digital di sektor perbankan membawa kemudahan, tetapi juga meningkatkan risiko ancaman siber. Ancaman seperti hacking, phishing, dan malware menjadi tantangan serius yang dapat merusak integritas sistem perbankan dan membahayakan data nasabah. Oleh karena itu, perlindungan data nasabah harus menjadi prioritas utama bagi lembaga keuangan. Kesadaran akan pentingnya keamanan siber perlu ditingkatkan di semua level, baik dari pihak bank maupun nasabah.

Saran

Saran pertama adalah meningkatkan edukasi keamanan siber bagi nasabah. Bank perlu menyediakan pelatihan dan informasi yang jelas tentang cara melindungi data pribadi mereka. Dengan pengetahuan yang lebih baik, nasabah dapat lebih waspada terhadap potensi penipuan dan ancaman yang ada. Kedua, bank harus mengadopsi teknologi keamanan terbaru. Penerapan sistem enkripsi dan otentikasi dua faktor dapat memberikan lapisan perlindungan tambahan terhadap data sensitif. Selain itu, penggunaan kecerdasan buatan untuk mendeteksi pola serangan siber secara real-time dapat membantu dalam mencegah kerugian yang lebih besar. Ketiga, kolaborasi antara bank dan regulator sangat penting. Kerjasama ini dapat menciptakan standar keamanan yang lebih ketat dan memastikan bahwa semua lembaga keuangan mematuhi regulasi yang ada. Hal ini tidak hanya akan melindungi data nasabah tetapi juga meningkatkan kepercayaan masyarakat terhadap sistem perbankan. Keempat, bank perlu melakukan audit keamanan secara berkala untuk mengidentifikasi celah dalam sistem mereka. Dengan melakukan evaluasi rutin, bank dapat memperbaiki kelemahan sebelum dimanfaatkan oleh penjahat siber. Ini juga mencakup pemantauan aktivitas pegawai untuk mencegah ancaman dari dalam. Dengan langkah-langkah ini, diharapkan sektor perbankan dapat menciptakan lingkungan yang lebih aman bagi nasabah di era digital. Perlindungan data bukan hanya tanggung jawab bank, tetapi juga melibatkan partisipasi aktif dari nasabah untuk menjaga keamanan informasi pribadi mereka.

DAFTAR PUSTAKA

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan. *HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis*, *2*(7), 692–700.

Delvyan Putri Surya Ningrum, & Jamiatur Robekha. (2023). Analisa Yuridis Dalam Kasus

Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4), 765–776. https://doi.org/10.56799/peshum.v2i4.2115

Fanasafa I. (2022). *Waspada! Kejahatan Phising Mengintai Anda*. https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html, diakses pada tanggal 21 November 2024.

Ghozali, M., Liana, N., Afra, C., Siregar, Z., Nurfahni, Malahayati, & Hatta, M. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *CENDEKIA: Jurnal Hukum, Sosial & Humaniora*, *2*(4), 797–809.

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, *1*(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Sembiring, E. R. M., Nurbaiti, N., & Daulay, A. N. (2024). Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada. *Manajemen Pendidikan Dan Ilmu Sosial (JMPIS)*, *5*(4), 880–887.