KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.1 Februari 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 432-440
DOI: https://doi.org/10.61722/jmia. v2i1.3383

Analisis Kasus Bank Jago: Eks Karyawan Bobol 112 Rekening Nasabah Senilai Rp1,39 Miliar melalui Pembukaan Blokir Ilegal

Faza Fatkhun Nadhif
Fakultas Hukum Universitas Negeri Semarang
Muhammad Rizki Meidianto
Fakultas Hukum Universitas Negeri Semarang
Yusuf Suprayogi
Fakultas Hukum Universitas Negeri Semarang
Mahesya Ayu Rahman
Fakultas Hukum UPN Veteran Jakarta
William Putra Hatorangan
Fakultas Hukum UPN Veteran Jakarta

Alamat Unnes: Sekaran, Gunung Pati, Kota Semarang, Jawa Tengah 50229
Alamat UPN Veteran Jakarta: Jalan RS. Fatmawati Raya, Pondok Labu, Cilandak, Kota Jakarta Selatan, Jakarta 12450
Korespondensi penulis: fazanadhif29@students.unnes.ac.id

Abstrak. *The case of the burglary of 112 Bank Jago customer accounts by a former employee with losses reaching IDR 1.39 billion reflects a serious threat to the security of the digital banking system. The mode of crime in the form of illegally opening blocking of accounts by perpetrators who have special access indicates weaknesses in internal supervision and system security. This research aims to identify weak factors in Bank Jago's security system, the role of law enforcement officers (APH) in handling this case, as well as the legal implications for the bank's responsibilities. The approach used is a qualitative method with descriptive analysis of secondary data, including banking regulations, case reports and related publications. The analysis results show that the main weaknesses lie in the lack of internal supervision, unlimited system access, a vulnerable security system, and suboptimal authentication and activity monitoring mechanisms. APH's role has proven to be crucial in detecting and handling cases, including making arrests, confiscating evidence, and preparing legal cases. This case provides important lessons for the banking industry to strengthen security policies, including implementing multi-factor authentication, monitoring log activity, and regular audits. In addition, cooperation between banks and legal authorities must be improved to mitigate similar risks in the future. This strategy not only aims to protect customers but also restore public trust in digital banking services.*
Keywords: *internal Crime; Digital Banking Cecurity; Internal Supervision; Legal Responsibility; Bank Jago.*

Abstrak. Kasus pembobolan 112 rekening nasabah Bank Jago oleh seorang eks karyawan dengan kerugian mencapai Rp1,39 miliar mencerminkan ancaman serius terhadap keamanan sistem perbankan digital. Modus kejahatan berupa pembukaan blokir rekening secara ilegal oleh pelaku yang memiliki akses khusus mengindikasikan kelemahan pengawasan internal dan keamanan sistem. Penelitian ini bertujuan untuk mengidentifikasi faktor kelemahan dalam sistem keamanan Bank Jago, peran aparat penegak hukum (APH) dalam menangani kasus ini, serta implikasi hukum terhadap tanggung jawab bank. Pendekatan yang digunakan adalah metode kualitatif dengan analisis deskriptif terhadap data sekunder, termasuk regulasi perbankan, laporan kasus, dan publikasi terkait. Hasil analisis menunjukkan bahwa kelemahan utama terletak pada kurangnya pengawasan internal, akses sistem yang tidak terbatas, sistem keamanan yang rentan, serta mekanisme otentikasi dan pemantauan aktivitas yang tidak optimal. Peran APH terbukti krusial dalam mendeteksi dan menangani kasus, termasuk melakukan penangkapan, penyitaan bukti, dan penyusunan perkara hukum. Kasus ini memberikan pembelajaran penting bagi industri perbankan untuk memperkuat kebijakan keamanan, meliputi penerapan otentikasi multi-faktor, pemantauan aktivitas log, dan audit reguler. Selain itu, kerjasama antara bank dan aparat hukum harus ditingkatkan untuk memitigasi

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

risiko serupa di masa depan. Strategi ini tidak hanya bertujuan melindungi nasabah tetapi juga memulihkan kepercayaan masyarakat terhadap layanan perbankan digital

Kata Kunci: *Kejahatan Internal, Keamanan Perbankan Digital, Pengawasan Internal, Tanggung Jawab Hukum, Bank Jago*

PENDAHULUAN

Eks karyawan Bank Jago telah membobol 112 rekening nasabah dengan dana sebesar Rp1,39 miliar.Tersangka berinisial IA disebut telah melakukan pembukaan blokir secara ilegal terhadap akun rekening nasabah Bank Jago yang telah diblokir berdasarkan permintaan APH (Aparat Penegak Hukum) karena terindikasi menerima aliran dana hasil tindak pidana.Dari perbuatannya, Tersangka diketahui telah melakukan 112 approval pembukaan blokir rekening Bank Jago dengan total uang yang dipindahkan sebesar Rp1.397.280.711 yang kemudian dialihkan ke rekening penampungan yang telah disiapkan oleh Tersangka. peristiwa ini menunjukkan bahwa ancaman kejahatan siber tidak hanya datang dari pihak luar, tetapi juga dapat dilakukan oleh orang dalam yang memiliki akses khusus ke sistem bank. Modus kejahatan berupa pembukaan blokir rekening secara ilegal ini mengindikasikan adanya celah dalam sistem keamanan, padahal proses perbankan seharusnya menjunjung tinggi prinsip transparansi, akuntabilitas, dan perlindungan terhadap hak nasabah.

Seiring dengan berkembangnya digitalisasi di sektor perbankan, kasus ini menegaskan pentingnya penguatan sistem keamanan, baik melalui teknologi yang lebih andal maupun manajemen sumber daya manusia yang lebih ketat. Selain itu, peristiwa ini menimbulkan

Pertanyaan serius terkait tanggung jawab hukum bank atas kerugian yang dialami nasabah akibat kelalaian pengawasan internal. Kajian mendalam terhadap kasus ini tidak hanya akan mengungkap akar masalah dan dampaknya, tetapi juga dapat menjadi dasar untuk merancang strategi pencegahan kejahatan serupa di masa depan. Langkah-langkah ini penting untuk memulihkan dan memperkuat kepercayaan masyarakat terhadap keamanan layanan perbankan digital. Kasus pembobolan rekening nasabah oleh eks karyawan Bank Jago dengan total kerugian Rp1,39 miliar menjadi salah satu bukti nyata bahwa ancaman terhadap sistem perbankan digital semakin kompleks. Tindakan pembukaan blokir rekening secara ilegal oleh orang dalam ini menyoroti pentingnya evaluasi menyeluruh terhadap kebijakan pengelolaan akses dan pengawasan internal di institusi keuangan. Modus operandi yang melibatkan penggunaan akses khusus karyawan untuk memanipulasi data nasabah menunjukkan bahwa celah keamanan tidak hanya bersumber dari serangan eksternal seperti peretasan, tetapi juga dari kurangnya pengendalian terhadap akses internal. Situasi ini memunculkan urgensi untuk memperkuat kebijakan perlindungan sistem perbankan digital.

Selain dari aspek keamanan teknis, peristiwa ini menggarisbawahi perlunya peningkatan kapasitas manajemen risiko melalui pengawasan berbasis teknologi serta

pelatihan karyawan secara berkala. Dengan semakin tingginya adopsi teknologi digital di sektor perbankan, setiap bank, termasuk Bank Jago, dituntut untuk memastikan bahwa teknologi yang digunakan mampu mengakomodasi prinsip keamanan siber modern, seperti otentikasi multi-faktor, pencatatan log aktivitas yang akurat, serta pembatasan akses berdasarkan peran (*role-based access control*). Langkah-langkah ini sangat penting untuk mencegah potensi penyalahgunaan sistem oleh pihak internal yang memiliki akses tinggi. Lebih jauh, kasus ini memunculkan implikasi hukum yang signifikan. Kegagalan pengawasan internal yang berujung pada kerugian nasabah membuka ruang untuk mempertanyakan tanggung jawab bank sebagai penyedia layanan keuangan. Sesuai dengan undang-undang perbankan, bank memiliki kewajiban untuk melindungi data dan dana nasabah dari segala bentuk ancaman, termasuk kejahatan internal. Oleh karena itu, institusi perbankan harus memastikan bahwa kebijakan dan prosedur mereka tidak hanya mematuhi regulasi yang berlaku, tetapi juga mampu melindungi kepentingan nasabah secara menyeluruh.

Pendekatan yang menyeluruh terhadap permasalahan ini dapat mencakup tiga elemen utama: perbaikan kebijakan internal, peningkatan kapasitas teknologi, dan kolaborasi yang lebih erat dengan aparat penegak hukum. Kajian mendalam terhadap insiden ini juga memberikan peluang untuk merumuskan strategi pencegahan jangka panjang yang dapat diterapkan oleh industri perbankan secara umum. Dengan langkah yang tepat, kasus ini dapat menjadi pembelajaran penting untuk memperkuat kepercayaan masyarakat terhadap sistem perbankan digital yang aman dan andal.

KAJIAN TEORI

Bagian ini menguraikan teori-teori relevan yang mendasari topik penelitian dan memberikan ulasan tentang beberapa penelitian sebelumnya yang relevan dan memberikan acuan serta landasan bagi penelitian ini dilakukan. Jika ada hipotesis, bisa dinyatakan tidak tersurat dan tidak harus dalam kalimat tanya.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitis. Pendekatan ini digunakan untuk mendalami isu konflik kepentingan antara kerahasiaan data nasabah dan hak atas informasi, serta untuk memahami dan menganalisis pengaturan hukum yang relevan di Indonesia. Proses penelitian dilakukan melalui pengumpulan data sekunder yang meliputi dokumen hukum, literatur akademik, laporan penelitian sebelumnya serta publikasi resmi dari institusi terkait. dan analisis data secara sistematis, dengan tujuan menghasilkan rekomendasi. Penelitian ini berfokus pada pengaturan hukum di indonesia dengan analisis terhadap lembaga perbankan nasional, regulasi sektor keuangan dan sistem hukum yang berlaku.

HASIL PENELITIAN DAN PEMBAHASAN

PEMBAHASAN

1. Peran Aparat Penegak Hukum Dalam Kasus Pembobolan Rekening Nasabah di Bank Jago

Kasus ini berawal dari laporan yang diajukan pada 31 Oktober 2023 oleh salah satu kuasa korban, Rio Franstedi, terkait dugaan pelanggaran akses sistem Bank Jago. Laporan tersebut mengungkapkan bahwa sejak 18 Maret 2023 hingga 31 Oktober 2023, telah terjadi tindak kejahatan yang melibatkan pihak terduga berinisial "IA" (23 tahun). Dalam laporan tersebut, pihak korban menyatakan bahwa terduga telah mengakses sistem Bank Jago dan melakukan aktivitas ilegal.

Dugaan kejahatan yang dilakukan oleh terlapor mencakup pembukaan 112 akun rekening nasabah yang sebelumnya terblokir. Akun-akun tersebut kemudian digunakan oleh terlapor untuk melakukan transaksi yang tidak sah. Terlapor diketahui dengan sengaja mengambil dana dari rekening nasabah yang terblokir dan langsung memindahkannya ke rekening penampung yang telah dipersiapkan oleh pelaku.

Pelaku diketahui dapat membuka rekening nasabah yang telah diblokir karena ia merupakan pegawai Bank Jago. Dalam kapasitasnya sebagai Spesialis Pusat Kontak Bank Jago (Contact Center Specialist), pelaku memiliki kewenangan untuk mengajukan permintaan pembukaan blokir melalui Pusat Komando Agen (Agent Command Center). Permintaan tersebut disetujui oleh sistem karena termasuk dalam wewenangnya sebagai pegawai. Pelaku memanfaatkan akses ini untuk melakukan tindakan ilegal.

Menurut pihak Bank Jago, rekening-rekening yang diblokir dan diakses oleh pelaku (IA) terindikasi terkait tindak pidana, termasuk penipuan, pencucian uang, hingga aktivitas terorisme. Menanggapi laporan ini, pada 4 Juli 2024 pukul 00.50 WIB, tim penyidik melakukan tindakan penangkapan terhadap pelaku di Kecamatan Ciputat Timur, Tangerang Selatan. Saat penangkapan, penyidik juga mengamankan barang bukti berupa dua unit ponsel dan log akses yang menunjukkan pembukaan 112 rekening yang terindikasi digunakan untuk aktivitas penipuan oleh pelaku.

Dari hasil penyelidikan, diketahui bahwa tindakan pelaku telah menyebabkan kerugian besar bagi Bank Jago, yang diperkirakan mencapai Rp1.397.280.711. Dana hasil kejahatan tersebut diduga digunakan oleh pelaku untuk membayar utang pribadi serta membiayai perjalanan liburan.

Kasus ini mencerminkan adanya indikasi pelanggaran serius terhadap regulasi di sektor perbankan, khususnya terkait perlindungan konsumen dan keamanan data pribadi nasabah. Situasi ini menjadi titik kritis bagi Bank Jago, yang seharusnya bertanggung jawab menjaga kerahasiaan informasi keuangan nasabahnya. Hal ini merujuk pada Pasal 2 Undang-Undang Nomor 23 PrP Tahun 1960 tentang Bank, yang menyatakan, *"Bank tidak boleh memberikan keterangan-keterangan tentang keadaan keuangan langganannya yang tercatat padanya dan hal-hal lain yang harus dirahasiakan dalam dunia perbankan."*

Definisi mengenai rahasia bank juga diatur dalam Pasal 1 angka (16) Undang-Undang Nomor 7 Tahun 1992 sebagaimana telah diubah oleh Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Ketentuan tersebut menjelaskan bahwa *"Rahasia Bank adalah segala sesuatu yang berhubungan dengan keuangan dan hal-hal lain dari nasabah bank yang menurut kelaziman dunia perbankan wajib dirahasiakan."* Pelanggaran terhadap prinsip ini tidak hanya merugikan nasabah, tetapi juga mencoreng reputasi dunia perbankan secara keseluruhan.

Aparat penegak hukum berperan krusial dalam mendeteksi dan menindaklanjuti laporan mengenai penyalahgunaan hak akses yang terjadi di Bank Jago. Kasus ini terungkap setelah laporan dari pihak bank kepada Polda Metro Jaya pada 7 Desember 2023, yang menyatakan bahwa ada dugaan penyalahgunaan hak akses terhadap sistem bank oleh IA. Tindakan ini melibatkan pembukaan blokir rekening yang seharusnya tetap terblokir berdasarkan permintaan APH karena terindikasi menerima dana hasil tindak pidana.

Pihak kepolisian, melalui Direktur Reserse Kriminal Khusus Polda Metro Jaya, Kombes Pol Ade Safri Simanjuntak, menjelaskan bahwa IA berhasil membuka blokir 112 rekening dan memindahkan dana sebesar Rp1,39 miliar ke rekening penampungan yang telah disiapkan sebelumnya. Penangkapan IA dilakukan pada 4 Juli 2024 setelah penyidik mengumpulkan bukti dan melakukan investigasi lebih lanjut.

Proses Hukum dan Penegakan Hukum. Setelah penangkapan, aparat penegak hukum bertanggung jawab untuk melanjutkan proses hukum terhadap tersangka. Ini termasuk penyitaan barang bukti, seperti ponsel dan log akses yang digunakan untuk melakukan pembobolan. Selain itu, polisi juga akan berkoordinasi dengan jaksa penuntut umum untuk menyusun berkas perkara yang lengkap agar kasus ini dapat diajukan ke pengadilan.

Proses ini mencerminkan komitmen APH untuk menegakkan hukum dan memberikan efek jera kepada pelaku kejahatan finansial. Dengan menangkap tersangka dan memprosesnya secara hukum, APH menunjukkan bahwa tindakan kriminal dalam sektor perbankan tidak akan ditoleransi.

Kerjasama dengan Institusi Keuangan. Bank Jago juga menunjukkan peran aktif dalam kerjasama dengan aparat penegak hukum. Manajemen bank mengklaim bahwa mereka telah menerapkan langkah-langkah mitigasi risiko dan strategi anti-fraud untuk mencegah kejadian serupa di masa depan. Hal ini termasuk deteksi dini terhadap tindakan fraud dan pelaporan proaktif kepada pihak kepolisian.

Kerjasama ini sangat penting karena membantu memperkuat sistem keamanan perbankan serta meningkatkan kepercayaan nasabah terhadap institusi keuangan. Bank Jago menegaskan bahwa tidak ada nasabah yang dirugikan akibat tindakan IA, berkat langkah-langkah preventif yang telah diambil.

2. Faktor Kelemahan Dalam Sistem Keamanan Bank Jago Yang Memungkinkan Terjadinya Pembobolan Rekening Oleh Pihak Internal

Bank Digital diharapkan mampu menerapkan prinsip mengenal nasabah serta penerapan keamanan digital yang baik,pada hal ini Bank Jago dihadapkan dengan kebobolan nya sistem yang ada dalam bank jag, bank diwajibkan mampu terbuka kepada nasabah terkait data, informasi, dan atau hubungan usaha publik, Bank Digital diharapkan mampu menyelenggarakan teknologi dengan efektif berkaitan dengan inovatif. Demi kelancaran pencapaian tujuan dan kewajiban perlindungan nasabah, Bank Digital diwajibkan mampu memastikan kepatuhan terhadap ketentuan-ketentuan yang berlaku serta meningkatkan efektivitas pengawasan berbasis teknologi dengan memperhatikan 3 objek penting pelaksanaan perlindungan dalam hal ini Pelaporan, regulasi dan pengawasan. Dengan tetap memperhitungkan terkait kepentingan nasional dan perekonomian terkhusus pada perbankan dan keuangan digital dengan prinsip Resiprokalitas. Menurut Siagian (2008), faktor-faktor strategis dalam analisis dapat dibagi menjadi beberapa kategori:

Faktor Kekuatan: Merupakan keunggulan yang dimiliki oleh suatu perusahaan, termasuk unit-unit bisnis di dalamnya. Kekuatan ini meliputi kompetensi khusus yang memberikan keunggulan komparatif di pasar. Setiap unit bisnis memiliki sumber daya, keterampilan, atau produk unggulan yang membuatnya lebih mampu memenuhi kebutuhan pasar dibandingkan para pesaingnya.Faktor Kelemahan: Merujuk pada keterbatasan atau kekurangan dalam sumber daya, keterampilan, atau kemampuan yang dapat menghambat kinerja organisasi secara optimal.Faktor Peluang: Peluang adalah situasi lingkungan yang memberikan keuntungan bagi suatu unit bisnis atau organisasi.Faktor Ancaman: Berlawanan dengan peluang, ancaman mencakup faktor-faktor lingkungan yang tidak menguntungkan. Jika tidak ditangani, ancaman ini dapat menjadi hambatan atau bahaya bagi kelangsungan unit bisnis, baik saat ini maupun di masa mendatang.Pengetahuan masyarakat tentang teknologi finansial masih rendah, sehingga menghambat optimalisasi akses terhadap layanan keuangan perbankan.Ancaman keamanan siber, privasi, dan kepemilikan data, serta potensi penyalahgunaan data oleh pihak yang tidak bertanggung jawab menjadi risiko yang harus dihadapi.Ketidakmerataan infrastruktur teknologi informasi di berbagai wilayah Indonesia menyebabkan kesenjangan dalam akses layanan perbankan.Koneksi internet yang belum memadai, baik dari segi kecepatan, stabilitas server, maupun sistem aplikasi, masih menjadi kendala dalam mengelola transaksi data keuangan secara efisien.

1. Kurangnya Pengawasan Internal

Jika mekanisme pengawasan terhadap aktivitas karyawan tidak dijalankan secara rutin dan sistematis, pihak internal dengan niat buruk dapat memanfaatkan kelonggaran ini untuk mengakses atau memanipulasi rekening nasabah.

Contoh: Tidak adanya audit reguler terhadap aktivitas karyawan di sistem dapat membuat tindakan mencurigakan tidak terdeteksi.

Solusi:

Implementasi pengawasan berbasis teknologi, seperti *real-time monitoring*, untuk mencatat dan menganalisis setiap aktivitas pengguna.

Melakukan audit secara berkala terhadap semua akses dan transaksi.

2. Akses yang Tidak Terbatas

Karyawan yang memiliki akses terlalu luas ke sistem atau data nasabah dapat menyalahgunakannya untuk keuntungan pribadi.

Tidak adanya kebijakan *role-based access control* (RBAC) memungkinkan setiap pengguna memiliki hak yang tidak sesuai dengan tugas dan tanggung jawabnya.

Solusi:

Memberlakukan hak akses berbasis kebutuhan (prinsip *least privilege*) agar karyawan hanya dapat mengakses data atau sistem yang relevan dengan tugas mereka.

Memperkuat mekanisme pencatatan akses untuk mengetahui siapa yang mengakses data tertentu dan kapan akses dilakukan.

3. Sistem Keamanan yang Rentan

Jika sistem keamanan tidak dilengkapi dengan proteksi berlapis seperti enkripsi data, firewall canggih, atau *intrusion detection system (IDS)*, pihak internal dapat lebih mudah mengeksploitasi celah keamanan.

Contoh: Data rekening nasabah yang tidak terenkripsi rentan terhadap pencurian atau manipulasi.

Solusi:

Menggunakan sistem keamanan berlapis, termasuk enkripsi data, *intrusion detection*, dan *intrusion prevention systems*. Memastikan perangkat lunak yang digunakan selalu diperbarui untuk menghindari eksploitasi kerentanan.

4. Kelemahan dalam Proses Otentikasi

Sistem otentikasi yang hanya menggunakan kata sandi (password) tanpa lapisan keamanan tambahan rentan terhadap penyalahgunaan. Karyawan internal dapat menggunakan kredensial orang lain untuk mengakses data yang tidak seharusnya mereka lihat.

Solusi:

Menerapkan otentikasi multi-faktor (MFA) seperti kombinasi kata sandi, token, atau sidik jari. Melakukan evaluasi keamanan kata sandi secara berkala untuk memastikan pengguna tidak menggunakan kata sandi yang mudah ditebak.

5. Kurangnya Pemantauan Aktivitas Log

Sistem yang tidak mencatat atau memantau aktivitas log pengguna secara detail akan kesulitan mendeteksi perilaku mencurigakan dari pihak internal. Tanpa log aktivitas, tidak ada jejak yang bisa ditelusuri jika terjadi pembobolan.

Solusi:

Mengaktifkan sistem log yang mencatat semua aktivitas karyawan di dalam sistem, termasuk akses, perubahan data, atau transaksi. Menyediakan analisis log secara otomatis dengan *machine learning* untuk mendeteksi pola mencurigakan.

KESIMPULAN

Kasus pembobolan rekening nasabah di Bank Jago mengungkap kelemahan serius dalam sistem keamanan dan pengawasan internal perbankan. Tindak kejahatan yang dilakukan oleh salah satu pegawai bank menunjukkan adanya celah dalam pengendalian akses, otentikasi, dan pemantauan aktivitas karyawan. Hal ini diperparah oleh kurangnya penerapan sistem keamanan berlapis dan kebijakan berbasis peran (*role-based access control*). Selain itu, kasus ini juga menyoroti pentingnya peran aparat penegak hukum dalam mendeteksi, menangani, dan memberikan efek jera terhadap pelaku kejahatan di sektor perbankan. Proses hukum yang dilakukan oleh pihak kepolisian terhadap pelaku menunjukkan komitmen dalam menjaga kepercayaan masyarakat terhadap sistem keuangan. Di sisi lain, Bank Jago sebagai institusi keuangan digital harus lebih aktif memperkuat mekanisme keamanan, baik melalui teknologi, pengawasan internal, maupun pelatihan karyawan, untuk mencegah kejadian serupa di masa depan. Kerjasama erat antara institusi perbankan dan aparat penegak hukum menjadi kunci untuk menjaga integritas, melindungi data nasabah, dan memitigasi risiko kejahatan finansial secara menyeluruh. Dengan demikian, perbaikan yang berkelanjutan diperlukan untuk memastikan keamanan sistem perbankan dan mempertahankan kepercayaan publik.

SARAN

Pertama, Bank Jago dan institusi keuangan lainnya perlu segera memperkuat sistem keamanan digital mereka dengan menerapkan otentikasi multi-faktor, enkripsi data, dan teknologi deteksi intrusi yang canggih. Kebijakan pembatasan akses berbasis peran (*role-based access control*) juga harus diimplementasikan untuk memastikan bahwa karyawan hanya memiliki akses sesuai dengan tanggung jawab mereka. Kedua, pengawasan internal harus diperketat dengan

sistem monitoring aktivitas karyawan secara real-time untuk mendeteksi pola mencurigakan lebih dini. Ketiga, Bank Jago perlu menyelenggarakan pelatihan berkala bagi seluruh karyawan terkait keamanan data, etika kerja, dan pengelolaan risiko kejahatan internal. Selain itu, penting bagi Bank Jago untuk terus menjalin kerjasama erat dengan aparat penegak hukum dalam mengidentifikasi dan menangani potensi kejahatan finansial. Institusi keuangan juga dapat berkontribusi dalam pengembangan pedoman keamanan yang relevan bersama otoritas terkait guna menghadapi ancaman yang semakin kompleks. Langkah-langkah perbaikan ini harus dilakukan secara berkelanjutan agar keamanan sistem perbankan tetap terjaga, integritas institusi dapat dipertahankan, dan kepercayaan masyarakat terhadap sektor perbankan digital semakin meningkat.

DAFTAR PUSTAKA

Sitorus, Hany Ayunda Mernisi. “Perlindungan Hukum Terhadap Nasabah Atas Fraud Pada Transaksi Bank Digital.” *Jurnal Ilmu Sosial dan Pendidikan (JISIP)*, vol. 7, 2023. Accessed 16 12 2024.

Siagian, S. P. (2008). Manajemen Stratejik. Jakarta: Bumi Aksara.

Marginingsih, Ratnawaty. “Analisis SWOT Technology Financial (FinTech) Terhadap Industri Perbankan.” *Cakrawala-Jurnal Humaniora*, vol. 19, no. 1, 2019. Accessed 16 12 2024.

Haryono, S., & Widodo, P. (2020). "Implementasi Keamanan Siber dalam Meningkatkan Kepercayaan Nasabah Perbankan Digital." *Jurnal Manajemen & Bisnis Digital*, 7(2), 123–136.

Putri, A. P., & Pratama, A. (2021). "Analisis Kebijakan Perlindungan Konsumen pada Sistem Perbankan Digital di Indonesia." *Jurnal Hukum dan Keuangan*, 10(4), 211–230.

Setiawan, I., & Rahman, F. (2023). "Manajemen Risiko Keamanan Informasi pada Perbankan Digital: Studi Kasus Bank Digital di Indonesia." *Journal of Financial and Banking Technology*, 5(1), 45–61.

Wijaya, R., & Ardiansyah, D. (2022). "Peran Internal Audit dalam Mencegah Fraud di Industri Perbankan." *Jurnal Akuntansi dan Keuangan Indonesia*, 18(3), 275–290.

Sari, M., & Ahmad, S. (2019). "Efektivitas Otentikasi Multi-Faktor dalam Sistem Keamanan Perbankan." *Jurnal Teknologi Informasi dan Keamanan Siber*, 9(1), 88–101.

Buku

Arifin, Zainal. (2020). *Keamanan dan Risiko dalam Sistem Perbankan Digital*. Jakarta: Gramedia Pustaka Utama.

Siagian, Sondang P. (2019). *Manajemen Strategis: Konsep, Aplikasi, dan Implikasinya dalam Era Digital*. Bandung: Alfabeta.

Nugroho, Benny. (2021). *Cybersecurity dalam Dunia Perbankan*. Surabaya: Penerbit Erlangga.

Tambunan, Tulus T.H. (2022). *Digitalisasi di Sektor Keuangan: Peluang, Risiko, dan Tantangan di Indonesia*. Jakarta: UI Press.

Rivai, Veithzal. (2019). *Manajemen Risiko Perbankan: Teori dan Implementasi*. Jakarta: Rajawali Pers.