Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

Oktober 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 180-186

Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi Dalam Sistem Perbankan

Ardita Esti Rahmadani[1], Yoga Pangestu[2], Nur Halizhah[3]
[123]Ilmu Hukum Fakultas Hukum Universitas Negri Semarang
Email: estardita@gmail.com[1], yogapengestu243@gmail.com[2], nrrhalizhah@gmail.com[3]

Abstract
Artikel ini membahas tantangan dan solusi perlindungan data pribadi di sektor perbankan di era digital. Kemajuan teknologi informasi memberikan kemudahan akses namun juga meningkatkan risiko keamanan data nasabah, termasuk peretasan, pencurian identitas, dan pelanggaran privasi. Penelitian ini menggunakan pendekatan deskriptif-analitis dengan metode kualitatif untuk mengeksplorasi tantangan utama yang dihadapi bank serta solusi yang dapat diterapkan, seperti teknologi enkripsi, sistem deteksi dan pencegahan intrusi, serta program edukasi literasi digital bagi nasabah. Dengan pendekatan ini, artikel menyajikan rekomendasi kebijakan dan teknologi bagi sektor perbankan untuk meningkatkan keamanan data nasabah di Indonesia.

Article History
Received Okt 17, 2024
Revised Okt 20, 2024
Accepted 29 Okt 2024
Available online 07 Nov. 2024

Keywords :
Perlindungan Data; Keamanan Siber; Literasi Digital.

Abstrak
This article discusses the challenges and solutions for personal data protection in the banking sector in the digital era. Advances in information technology provide ease of access but also increase the risk of data security breaches, including hacking, identity theft, and privacy violations. This study uses a descriptive-analytical approach with qualitative methods to explore the main challenges faced by banks and the solutions that can be applied, such as encryption technology, intrusion detection and prevention systems, and digital literacy education programs for customers. With this approach, the article presents policy and technological recommendations for the banking sector to enhance customer data security in Indonesia

Kata Kunci :
Data Protection; Cybersecurity; Digital Literacy

https://doi.org/10.5281/zenodo.14060556

This is an open-access article under the **CC-BY-SA License.**

PENDAHULUAN

Kemajuan teknologi informasi, terutama dalam bidang interkoneksi jaringan, telah memberikan pengaruh yang sangat signifikan terhadap berbagai aspek kehidupan manusia. [1]Perkembangan ini tidak hanya mempermudah komunikasi dan akses informasi, tetapi juga mengubah cara kita bekerja, belajar, dan berinteraksi. Sejak revolusi industri pada abad ke 18-20 , perkembangan teknologi telah mengalami percepatan yang luar biasa, membawa dampak signifikan pada ekonomi, sosial, dan budaya. Memasuki abad ke-21, perkembangan teknologi informasi dan komunikasi (TIK) telah menjadi pilar utama kemajuan teknologi. Internet, yang awalnya dikembangkan sebagai proyek militer pada tahun 1960-an, kini telah menjadi infrastruktur global yang menghubungkan miliaran orang di seluruh dunia. Teknologi informasi telah memungkinkan kita untuk terhubung dengan orang-orang di seluruh dunia dalam hitungan detik, mengakses informasi dari berbagai sumber dengan mudah, dan melakukan pekerjaan secara lebih efisien melalui berbagai alat dan platform digital.

Seiring dengan semakin meluasnya penggunaan internet, kebutuhan akan perlindungan data pribadi menjadi semakin mendesak. Data pribadi kini menjadi aset yang sangat berharga dan rentan terhadap berbagai ancaman, seperti peretasan, pencurian identitas, dan penyalahgunaan informasi. Setiap hari, jutaan data pribadi dikumpulkan, disimpan, dan diproses oleh berbagai entitas, mulai dari perusahaan teknologi besar hingga layanan online kecil. Hal ini menimbulkan risiko yang signifikan terhadap privasi dan keamanan data pribadi. Di era digital, data kini menjadi aset paling berharga bagi

[1] Maharani, R., & Prakoso, A. L. (2024). *Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital*. Jurnal USM Law Review, hlm. *7*(1), 333-347.

Oktober 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 180-186

organisasi dan individu. Data berfungsi sebagai sumber informasi yang sangat penting untuk pengambilan keputusan strategis, menciptakan nilai tambah bagi perusahaan, dan mendorong inovasi.[2]

Oleh karena itu, menjaga keamanan data menjadi hal yang sangat krusial dan penting dalam proses transformasi digital. Transformasi digital berkembang pesat di Indonesia, dengan pemerintah meluncurkan berbagai inisiatif untuk mempercepat proses ini. Inisiatif-inisiatif tersebut mencakup pengembangan infrastruktur digital, peningkatan literasi digital, dan penerapan teknologi baru di berbagai sektor. Namun, seiring dengan pesatnya perkembangan transformasi digital, masalah keamanan data telah menjadi isu yang sangat serius di seluruh dunia. Data pribadi dan informasi sensitif lainnya rentan terhadap berbagai ancaman, seperti peretasan, pencurian identitas, dan penyalahgunaan informasi. Data yang tidak terlindungi dengan baik dapat dilihat oleh pihak yang tidak berwenang dan digunakan untuk tujuan jahat, seperti penipuan, pemerasan, atau bahkan sabotase. Untuk mengatasi masalah ini, penting bagi organisasi dan individu untuk menerapkan langkah-langkah keamanan data yang komprehensif. Ini termasuk penggunaan teknologi enkripsi, kebijakan privasi yang ketat, dan pelatihan keamanan siber bagi karyawan. Selain itu, regulasi dan standar keamanan data yang ketat juga perlu diterapkan untuk memastikan bahwa data pribadi dilindungi dengan baik.

METODE PENULISAN

Metode penulisan dalam artikel ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis yang bertujuan untuk menggambarkan tantangan dan solusi dalam perlindungan data pribadi di sektor perbankan pada era digital. Penelitian ini dilakukan melalui kajian pustaka yang melibatkan berbagai sumber ilmiah, seperti buku, jurnal penelitian, artikel kebijakan, serta regulasi yang relevan, termasuk Undang-Undang Perlindungan Data Pribadi di Indonesia dan pedoman internasional terkait perlindungan data.[3] Metode ini dirancang untuk memberikan gambaran yang komprehensif mengenai tantangan utama yang dihadapi oleh sektor perbankan dalam menjaga keamanan data pribadi nasabah, seperti risiko peretasan, pencurian identitas, dan pelanggaran privasi yang dapat merusak kepercayaan nasabah.[4] Selain itu, kajian ini bertujuan untuk menganalisis solusi teknis dan kebijakan yang diterapkan, termasuk enkripsi data, penggunaan sistem deteksi intrusi, serta edukasi literasi digital untuk nasabah.

Selanjutnya, melalui pendekatan normatif, penelitian ini juga mengkaji aspek regulasi yang ada dalam rangka menilai efektivitas perlindungan data di Indonesia jika dibandingkan dengan standar internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa.[5] Analisis normatif ini dilakukan untuk melihat apakah regulasi di Indonesia telah memadai dalam menjamin keamanan data nasabah bank atau masih membutuhkan perbaikan, terutama dalam hal penerapan dan pengawasan.[6] Kajian ini diharapkan dapat memberikan kontribusi dalam pengembangan kebijakan yang lebih efektif untuk menjaga keamanan data nasabah di tengah perkembangan teknologi yang pesat. Dengan demikian, artikel ini berupaya untuk menyusun rekomendasi yang konkret bagi pihak perbankan, baik dari sisi teknologi maupun kebijakan, agar mampu meningkatkan kepercayaan masyarakat melalui perlindungan data yang lebih kuat.

HASIL DAN PEMBAHASAN

Tantangan dalam Perlindungan Data Pribadi di Sektor Perbankan

Di era digital, teknologi informasi telah menjadi bagian tak terpisahkan dalam kehidupan manusia, mengubah berbagai sektor, termasuk sektor perbankan. Kemajuan teknologi, seperti internet, cloud computing, dan big data, telah memungkinkan bank untuk memberikan layanan yang lebih cepat, efisien, dan mudah diakses oleh nasabah. Namun, dengan kemajuan tersebut muncul tantangan

[2] Satria, A., Ulina, N. P. H., Safira, P., & Pangestu, B. (2024). *"PERSPEKTIF HUKUM TERHADAP KEAMANAN DATA: TANTANGAN DAN SOLUSI DI ERA TEKNOLOGI INFORMASI"*. Warta Dharmawangsa, *18*(1), hlm. 177-192.
[3] Iqbal. (2020*). "Perlindungan Data Pribadi di Era Digital"*. hlm. 12.
[4] Setiawan & Wahyudi.(2019). *"Kebijakan Perlindungan Data di Sektor Perbankan"*. hlm. 25.
[5] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 15.
[6] Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 78.

Oktober 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 180-186

besar dalam hal keamanan data pribadi. Data nasabah perbankan, yang meliputi informasi finansial, riwayat transaksi, dan data identitas, kini menjadi aset berharga yang rentan terhadap berbagai ancaman keamanan. Meningkatnya penggunaan teknologi digital di sektor perbankan juga diiringi dengan lonjakan ancaman siber yang semakin canggih. Risiko pencurian identitas, peretasan data, dan penyalahgunaan informasi pribadi semakin tinggi, terutama karena data yang disimpan oleh bank mengandung nilai ekonomi yang sangat tinggi. Oleh karena itu, keamanan data pribadi telah menjadi perhatian utama bagi sektor perbankan, yang diharapkan dapat melindungi data nasabah secara efektif untuk menjaga kepercayaan publik.

Ancaman keamanan siber yang terus berkembang menjadi tantangan utama bagi perlindungan data di sektor perbankan. Bank menjadi target utama bagi para peretas karena data yang disimpan mengandung informasi keuangan bernilai tinggi. Serangan siber seperti phishing, ransomware, dan serangan malware semakin sering terjadi, yang dapat merusak sistem perbankan dan mengekspos data pribadi nasabah.[7] Selain itu, teknik peretasan semakin kompleks dan sulit untuk dideteksi, menyebabkan risiko kebocoran data semakin meningkat. Oleh karena itu, bank perlu menginvestasikan sumber daya yang signifikan dalam teknologi keamanan siber dan protokol perlindungan data untuk memitigasi ancaman ini.

Tantangan berikutnya datang dari rendahnya literasi digital di kalangan nasabah. Banyak nasabah perbankan yang tidak memiliki pengetahuan cukup mengenai risiko siber dan pentingnya menjaga keamanan data pribadi. Hal ini menjadikan mereka lebih rentan terhadap serangan social engineering, di mana pelaku kejahatan memanipulasi nasabah untuk memberikan informasi sensitif. Tanpa literasi digital yang memadai, nasabah cenderung menjadi target empuk bagi penipuan dan pencurian data.[8] Oleh karena itu, bank perlu melaksanakan program edukasi bagi nasabah mengenai praktik keamanan data yang baik, seperti tidak membagikan informasi login atau kata sandi dengan pihak ketiga.

Dalam operasionalnya, bank sering bekerja sama dengan berbagai pihak ketiga, seperti penyedia layanan teknologi, perusahaan fintech, dan vendor lainnya. Meski pihak ketiga ini memberikan nilai tambah bagi layanan bank, kolaborasi ini juga membawa risiko tambahan bagi keamanan data nasabah. Apabila pihak ketiga gagal menjaga standar keamanan yang sama ketatnya dengan bank, risiko kebocoran data semakin tinggi. Kebocoran data dari pihak ketiga dapat terjadi melalui serangan siber atau ketidakpatuhan pihak ketiga terhadap kebijakan perlindungan data yang ditetapkan bank. Bank perlu memastikan bahwa setiap mitra pihak ketiga telah memenuhi standar keamanan yang ketat dan melakukan audit secara berkala terhadap kepatuhan mereka dalam menjaga data nasabah.[9]

Perlindungan data pribadi di Indonesia masih menghadapi tantangan besar dari sisi regulasi. Meskipun pemerintah telah mengesahkan Undang-Undang Perlindungan Data Pribadi, penerapannya masih dalam tahap awal, dan masih ada beberapa kelemahan yang harus diperbaiki. Di negara-negara maju, regulasi perlindungan data pribadi telah mencakup aspek-aspek spesifik terkait perlindungan data di sektor perbankan, sementara di Indonesia regulasi yang berlaku masih umum dan membutuhkan spesifikasi lebih lanjut untuk sektor ini.[10] Selain itu, penegakan hukum yang lemah dan kurangnya mekanisme pengawasan yang efektif menjadi hambatan dalam perlindungan data nasabah. Bank di Indonesia dihadapkan pada tantangan untuk tetap patuh pada regulasi yang ada sambil memenuhi standar internasional dalam keamanan data.[11]

Solusi yang dapat diterapkan oleh bank untuk meningkatkan perlindungan data pribadi nasabah dan mengedukasi konsumen mengenai pentingnya menjaga data pribadi mereka

Dalam era digital yang semakin maju, data pribadi telah menjadi aset yang sangat berharga bagi individu dan organisasi. Bank, sebagai lembaga keuangan yang mengelola sejumlah besar data pribadi

[7] Krippendorff, K. (2019). "*The Cybersecurity Dilemma: Policy and Strategy in the Internet Era"*. Oxford University Press.
[8] Smith, A. (2020). *"Digital Literacy and Cybersecurity in the Financial Sector"*. Journal of Information Technology, 17(3), hlm. 85-98.
[9] Bellovin, S. M., & Schneier, B. (2017). *"Emerging Security Threats in Digital Banking"*. Financial Security Today, 6(2), hlm. 15-23.
[10] Dewi, R. (2021). *"Tantangan Hukum dalam Perlindungan Data di Sektor Perbankan Indonesia"* . Jurnal Hukum Indonesia, 12(3), hlm. 137-150.
[11] Setiawan, B. (2022). *"Memahami Hukum Perlindungan Data Pribadi Indonesia*". Jurnal Hukum dan Transformasi Digital, 4(1), hlm. 55-68.

Oktober 2024. Vol 2, No. 4
e-ISSN: 3032-6591
pp 180-186

nasabah, memiliki tanggung jawab besar untuk memastikan bahwa data tersebut terlindungi dengan baik. Perlindungan data pribadi tidak hanya penting untuk menjaga privasi nasabah, tetapi juga untuk membangun kepercayaan dan kredibilitas bank di mata masyarakat. Selain itu, edukasi kepada konsumen mengenai pentingnya menjaga data pribadi mereka juga menjadi aspek krusial dalam menciptakan lingkungan perbankan yang aman dan terpercaya. Beberapa hal yang dapat dilakukan bank agar mampu meningkatkan perlindungan data pribadi dan mengedukasi konsumen mengenai pentingnya menjaga data pribadi mereka, yaitu :

1. Enkripsi Data

Menggunakan teknologi enkripsi untuk melindungi data pribadi nasabah adalah langkah penting dalam menjaga keamanan informasi. Enkripsi bekerja dengan mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci dekripsi yang sah. Proses ini memastikan bahwa meskipun data berhasil dicuri oleh pihak yang tidak berwenang, informasi tersebut tetap tidak dapat diakses atau dimanfaatkan. Teknologi enkripsi dapat diterapkan pada berbagai jenis data, termasuk data yang disimpan di server, data yang dikirim melalui jaringan, dan data yang digunakan dalam aplikasi. Dengan menerapkan enkripsi, bank dapat memberikan lapisan perlindungan tambahan yang signifikan terhadap data pribadi nasabah, mengurangi risiko kebocoran data, dan meningkatkan kepercayaan nasabah terhadap keamanan layanan perbankan. Selain itu, enkripsi juga membantu bank mematuhi regulasi dan standar keamanan data yang ketat, memastikan bahwa data pribadi nasabah dilindungi sesuai dengan ketentuan hukum yang berlaku.[12]

2. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS)

Mengimplementasikan sistem deteksi dan pencegahan intrusi (IDS/IPS) adalah langkah penting dalam menjaga keamanan jaringan dan melindungi data pribadi nasabah. IDS/IPS bekerja dengan memonitor jaringan secara terus-menerus untuk mendeteksi aktivitas mencurigakan yang dapat mengindikasikan adanya upaya peretasan atau akses tidak sah[13]. Sistem ini menggunakan berbagai teknik analisis untuk mengidentifikasi pola-pola yang mencurigakan dan potensi ancaman sebelum mereka dapat merusak sistem atau mencuri data. Dengan adanya IDS/IPS, bank dapat mencegah akses tidak sah dan mengambil tindakan cepat untuk mengatasi ancaman yang terdeteksi, sehingga mengurangi risiko kebocoran data dan meningkatkan keamanan jaringan secara keseluruhan. Selain itu, IDS/IPS juga membantu bank mematuhi regulasi keamanan data yang ketat dan memastikan bahwa data pribadi nasabah dilindungi dengan baik. Implementasi IDS/IPS yang efektif memerlukan pemantauan yang berkelanjutan, pembaruan sistem secara berkala, dan pelatihan bagi tim keamanan siber untuk memastikan bahwa sistem ini dapat berfungsi dengan optimal dalam menghadapi berbagai ancaman siber yang terus berkembang.

3. Kebijakan Privasi yang Ketat

Menerapkan kebijakan privasi yang ketat adalah langkah penting untuk mengatur bagaimana data pribadi nasabah dikumpulkan, disimpan, dan digunakan. Kebijakan privasi ini harus mencakup persetujuan eksplisit dari nasabah sebelum data mereka dikumpulkan dan digunakan, memastikan bahwa nasabah memiliki kontrol penuh atas informasi pribadi mereka.[14] [15]Kebijakan ini juga harus menjelaskan dengan jelas tujuan pengumpulan data, bagaimana data akan digunakan, dan langkah-langkah yang diambil untuk melindungi data dari akses yang tidak sah. Selain itu, kebijakan privasi harus mencakup prosedur untuk mengakses, memperbarui, atau menghapus data pribadi nasabah sesuai dengan permintaan mereka. Dengan menerapkan kebijakan privasi yang ketat, bank dapat membangun kepercayaan nasabah, mematuhi regulasi perlindungan data yang berlaku, dan mengurangi risiko kebocoran data serta penyalahgunaan informasi pribadi. Kebijakan ini juga harus

[12] Azzahrah, B. T., Hamdi, M. N. R., Raynee, R. R., Layla Ni'matussa'idah, Z., & Subakdi, S. (2024). *"Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital: Studi Kasus dan Implementasi*". Jurnal Pendidikan Tambusai, 8(2), hlm. 23934-23943.
[13] Santoso, J. D. (2017). *"Keamanan Jaringan Menggunakan IDS/IPS Strataguard sebagai Layanan Kemanan Jaringan Terpusat"*. Sains Dan Teknologi Informasi, *3*(2), hlm. 56-68.
[14] Islamy, I. T., Agatha, S. T., Ameron, R., Fuad, B. H., Evan, E., & Rakhmawati, N. A. (2018). *"Pentingnya memahami penerapan privasi di era teknologi informasi"*. Jurnal Teknologi Informasi dan Pendidikan, *11*(2), hlm. 21-28.
[15] Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2024). *"PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL: TANTANGAN DAN SOLUSI"*. Meraja journal, *7*(2), hlm. 138-155.

Oktober 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 180-186

diperbarui secara berkala untuk menyesuaikan dengan perkembangan teknologi dan perubahan regulasi, memastikan bahwa perlindungan data pribadi tetap efektif dan relevan.

4. Audit Keamanan Berkala

Melakukan audit keamanan secara berkala adalah langkah penting untuk mengidentifikasi dan memperbaiki kelemahan dalam sistem keamanan data. Audit ini melibatkan pemeriksaan menyeluruh terhadap semua aspek sistem keamanan, termasuk perangkat keras, perangkat lunak, kebijakan, dan prosedur.[16] Dengan melakukan audit secara rutin, bank dapat memastikan bahwa langkah-langkah perlindungan data selalu up-to-date dengan perkembangan teknologi dan ancaman terbaru. Audit keamanan juga membantu mengidentifikasi potensi risiko dan celah keamanan yang mungkin tidak terlihat dalam operasi sehari-hari. Setelah kelemahan teridentifikasi, langkah-langkah perbaikan dapat segera diambil untuk mengurangi risiko kebocoran data dan meningkatkan keamanan sistem secara keseluruhan. Selain itu, audit keamanan juga membantu bank mematuhi regulasi dan standar keamanan data yang berlaku, memastikan bahwa data pribadi nasabah dilindungi dengan baik dan sesuai dengan ketentuan hukum yang berlaku. Dengan demikian, audit keamanan berkala menjadi bagian integral dari strategi perlindungan data yang efektif dan berkelanjutan.

5. Pelatihan Keamanan Siber untuk Karyawan

Memberikan pelatihan keamanan siber kepada karyawan adalah langkah penting untuk meningkatkan kesadaran dan pengetahuan mereka tentang pentingnya perlindungan data pribadi. Pelatihan ini dapat mencakup berbagai topik, seperti cara mengenali dan menghindari ancaman siber, termasuk phishing, malware, dan serangan social engineering. Selain itu, pelatihan juga harus mencakup prosedur yang harus diikuti dalam kasus kebocoran data, seperti langkah-langkah mitigasi, pelaporan insiden, dan pemulihan data. Dengan meningkatkan kesadaran dan pengetahuan karyawan tentang keamanan siber, bank dapat mengurangi risiko kebocoran data yang disebabkan oleh kesalahan manusia dan memastikan bahwa karyawan siap menghadapi berbagai ancaman siber. Pelatihan yang berkelanjutan dan teratur juga penting untuk memastikan bahwa karyawan selalu up-to-date dengan perkembangan terbaru dalam teknologi dan ancaman siber, sehingga mereka dapat melindungi data pribadi nasabah dengan lebih efektif.

SIMPULAN

Artikel ini menunjukkan bahwa tantangan dalam melindungi data pribadi di sektor perbankan semakin kompleks di era digital, di mana teknologi informasi telah menjadi kebutuhan mendasar dalam layanan keuangan. Meskipun perkembangan teknologi memungkinkan bank memberikan layanan yang lebih efisien dan terhubung secara luas, data nasabah menjadi lebih rentan terhadap berbagai risiko keamanan, seperti peretasan, pencurian identitas, dan penyalahgunaan informasi pribadi. Keberadaan ancaman siber yang semakin canggih, seperti serangan phishing, ransomware, dan malware, mengindikasikan bahwa data perbankan menjadi target bernilai tinggi bagi pelaku kejahatan. Selain itu, rendahnya literasi digital di kalangan nasabah membuat mereka rentan terhadap ancaman social engineering, di mana pelaku kejahatan mengeksploitasi informasi pribadi melalui manipulasi psikologis. Di samping itu, kolaborasi dengan pihak ketiga seperti penyedia teknologi dan fintech juga menambah kerentanan, mengingat pengelolaan data yang terlibat dalam kerjasama ini sering kali tidak berada di bawah kendali langsung bank.

Dari sisi regulasi, perlindungan data pribadi di Indonesia masih berada pada tahap awal implementasi, meskipun pemerintah telah mengesahkan Undang-Undang Perlindungan Data Pribadi. Perbandingan dengan standar internasional, seperti GDPR di Uni Eropa, menunjukkan bahwa regulasi di Indonesia masih perlu diperkuat, terutama dalam aspek pengawasan dan penegakan hukum. Penguatan ini sangat penting agar bank di Indonesia dapat memenuhi standar keamanan yang lebih tinggi dan menjaga kepercayaan publik terhadap layanan perbankan. Oleh karena itu, peningkatan keamanan data pribadi membutuhkan pendekatan komprehensif yang mencakup penguatan regulasi, peningkatan literasi digital nasabah, serta penerapan solusi teknologi yang mumpuni di lingkungan perbankan.

[16] Yuniarti, S. (2019). *"Perlindungan hukum data pribadi di Indonesia"*. Business Economic, Communication, and Social Sciences Journal (BECOSS), *1*(1), hlm. 147-154.

Oktober 2024. Vol 2, No. 4
e-ISSN: 3032-6591
pp 180-186

SARAN

1. Penerapan Teknologi Enkripsi yang Lebih Kuat. Bank perlu menerapkan teknologi enkripsi pada semua tahap pengelolaan data, baik dalam penyimpanan, pengiriman, maupun akses data nasabah. Enkripsi ini akan memastikan data yang dicuri tidak dapat dimanfaatkan oleh pihak tidak berwenang, memberikan lapisan keamanan tambahan terhadap ancaman peretasan.
2. Implementasi Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS). Bank harus menggunakan IDS/IPS untuk mendeteksi aktivitas mencurigakan di jaringan dan memblokir ancaman potensial secara real-time. Teknologi ini membantu mencegah serangan siber sebelum data sensitif terekspos, sehingga menjaga integritas sistem dan data nasabah.
3. Program Edukasi dan Literasi Digital untuk Nasabah. Bank perlu mengadakan program edukasi literasi digital yang komprehensif bagi nasabah. Program ini dapat mencakup sosialisasi terkait praktik keamanan data, cara mengenali serangan phishing, pentingnya kerahasiaan kata sandi, dan tips melindungi data pribadi agar nasabah lebih siap menghadapi risiko siber.
4. Pengawasan Ketat terhadap Mitra Pihak Ketiga. Kolaborasi bank dengan pihak ketiga seperti fintech dan penyedia teknologi perlu disertai dengan pengawasan ketat. Bank disarankan untuk menetapkan standar keamanan yang jelas dalam kontrak kerja, serta melakukan audit keamanan secara berkala untuk memastikan kepatuhan pihak ketiga dalam menjaga data nasabah.
5. Penguatan Regulasi Perlindungan Data Pribadi. Pemerintah diharapkan memperkuat regulasi terkait perlindungan data pribadi di Indonesia agar setara dengan standar internasional, seperti GDPR. Hal ini mencakup peningkatan penegakan hukum dan mekanisme pengawasan agar sektor perbankan memiliki panduan yang jelas dalam menjaga keamanan data pribadi nasabah.

REFERENSI

Azzahrah, B. T., Hamdi, M. N. R., Raynee, R. R., Layla Ni'matussa'idah, Z., & Subakdi, S. (2024). "Tantangan Pertahanan Dan Keamanan Data Cyber Dalam Era Digital: Studi Kasus Dan Implementasi". Jurnal Pendidikan Tambusai, 8(2), Hlm. 23934-23943.

Bellovin, S. M., & Schneier, B. (2017). "Emerging Security Threats In Digital Banking". Financial Security Today, 6(2), Hlm. 15-23.

Dewi, R. (2021). "Tantangan Hukum Dalam Perlindungan Data Di Sektor Perbankan Indonesia" . Jurnal Hukum Indonesia, 12(3), Hlm. 137-150.

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. Jurnal USM Law Review, Hlm. 7(1), 333-347.

Iqbal. (2020). "Perlindungan Data Pribadi Di Era Digital". Hlm. 12.

Islamy, I. T., Agatha, S. T., Ameron, R., Fuad, B. H., Evan, E., & Rakhmawati, N. A. (2018). "Pentingnya Memahami Penerapan Privasi Di Era Teknologi Informasi". Jurnal Teknologi Informasi Dan Pendidikan, 11(2), Hlm. 21-28.

Krippendorff, K. (2019). "The Cybersecurity Dilemma: Policy And Strategy In The Internet Era". Oxford University Press.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, Pasal 15.

Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 78.

Santoso, J. D. (2017). "Keamanan Jaringan Menggunakan IDS/IPS Strataguard Sebagai Layanan Kemanan Jaringan Terpusat". Sains Dan Teknologi Informasi, 3(2), Hlm. 56-68.

Satria, A., Ulina, N. P. H., Safira, P., & Pangestu, B. (2024). "Perspektif Hukum Terhadap Keamanan Data: Tantangan Dan Solusi Di Era Teknologi Informasi". Warta Dharmawangsa, 18(1), Hlm. 177-192.

Setiawan, B. (2022). "Memahami Hukum Perlindungan Data Pribadi Indonesia". Jurnal Hukum Dan Transformasi Digital, 4(1), Hlm. 55-68.

Setiawan & Wahyudi.(2019). "Kebijakan Perlindungan Data Di Sektor Perbankan". Hlm. 25.

Smith, A. (2020). "Digital Literacy And Cybersecurity In The Financial Sector". Journal Of Information Technology, 17(3), Hlm. 85-98.

Oktober 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 180-186

Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2024). "Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi". Meraja Journal, 7(2), Hlm. 138-155.

Yuniarti, S. (2019). "Perlindungan Hukum Data Pribadi Di Indonesia". Business Economic, Communication, And Social Sciences Journal (BECOSS), 1(1), hlm. 147-154.