(2024), 2 (1): 156–165 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

PERLINDUNGAN TERHADAP KONSUMEN DALAM KASUS KEBOCORAN DATA BANK SYARIAH INDONESIA

Anggi Muhammad Chandraca Hutagalung[1)], Nadia Rhaesa Marendra [2)], Asmak Ul Hosnah [3)].

Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia [123]

Correspondence

Email: anggigalung45@gmail.com [1], nadiamarendra20@gmail.com [2], asmak.hosnah@unpak.ac.id [3] No. Telp:

Submitted 3januari 2024 Accepted 9 januari 2024 Published 10 januari 2024

ABSTRACT

The recent service disruption incident at Bank Syariah Indonesia (BSI), which was allegedly caused by a ransomware cyberattack. This incident should be an important lesson for the banking sector in Indonesia. According to a cybersecurity observer, it is necessary to strengthen the digital defense system because cyber attacks are now increasingly complex and sophisticated.Not only BSI, previously, Bank Jatim and BRI Life also experienced hacking in 2021, with alleged leaks of customers' personal data to the internet. Even in 2022, Bank Indonesia also admitted to being a victim of a ransomware attack. This kind of attack can be overcome if the victim has adequate data backup. However, some hacker groups such as LockBit and Conti are known to steal target data before encrypting it and demanding a ransom.To protect the public from potential personal data leaks in the future, President Joko Widodo is expected to immediately establish a personal data protection agency in accordance with the Personal Data Protection Law. This agency will be responsible for conducting assessments and investigations when data leaks occur, enabling prosecution of institutions or companies that fail to protect people's personal data. In the event of a cyberattack and suspected leakage of customers' personal data, banks are expected to immediately notify the public so that people can take the necessary security measures. This research focuses on anticipatory efforts to prevent future cases of customer data breaches.

Keywords : ransomware, cybercrime.

ABSTRAK

insiden gangguan layanan yang baru-baru ini menimpa Bank Syariah Indonesia (BSI), yang diduga disebabkan oleh serangan siber ransomware. Kejadian ini seharusnya menjadi pembelajaran penting bagi sektor perbankan di Indonesia. Menurut seorang pengamat keamanan siber, diperlukan penguatan pada sistem pertahanan digital karena serangan siber kini semakin kompleks dan canggih. Tidak hanya BSI, sebelumnya, Bank Jatim dan BRI Life juga mengalami peretasan pada tahun 2021, dengan dugaan kebocoran data pribadi nasabah ke internet. Bahkan pada tahun 2022, Bank Indonesia juga mengakui menjadi korban serangan ransomware. Serangan semacam ini dapat diatasi jika korban memiliki cadangan data yang memadai. Namun, beberapa kelompok peretas seperti LockBit dan Conti diketahui mencuri data target sebelum mengenkripsi dan meminta uang tebusan. Untuk melindungi masyarakat dari potensi kebocoran data pribadi di masa depan, Presiden Joko Widodo diharapkan segera membentuk lembaga perlindungan data pribadi sesuai dengan UU Perlindungan Data Pribadi. Lembaga ini akan bertanggung jawab untuk melakukan penilaian dan investigasi saat terjadi kebocoran data, memungkinkan penuntutan terhadap lembaga atau perusahaan yang gagal melindungi data pribadi masyarakat. Jika terjadi serangan siber dan dugaan kebocoran data pribadi nasabah, perbankan diharapkan segera memberitahu publik agar orang-orang dapat mengambil langkah-langkah keamanan yang diperlukan. Penelitian ini difokuskan pada upaya antisipasi untuk mencegah kasus pembobolan data nasabah di masa depan.

Kata Kunci : ransomware, Kejahatan Siber.

Pendahuluan

Latar Belakang Masalah

Sungguh suatu kejadian yang mengguncang ketika Bank Syariah Indonesia mengalami serangan ransomware yang begitu masif. LockBit, sebagai geng ransomware penguasa pada kuartal pertama 2022, berhasil mencaplok sekitar 38% dari total serangan yang terjadi. Dengan berhasil mencuri data dari lebih dari 15 juta nasabah dan pegawai, termasuk nomor telepon, alamat, nama, informasi dokumen, jumlah isi rekening, nomor kartu, transaksi, dan lainnya, serangan ini memberikan dampak signifikan bagi bank dan nasabahnya[1].

Otoritas Jasa Keuangan (OJK) menekankan pentingnya aspek keamanan dan langkah-langkah mitigasi risiko siber yang mengacu pada praktik terbaik di dunia. Bank diwajibkan untuk melakukan latihan risiko siber dan melaporkan setiap insiden yang terjadi. Tindakan pidana peretasan sistem IT akan ditangani oleh pihak penegak hukum, baik nasional maupun transnasional. Setelah keadaan kembali normal, Bank Syariah Indonesia bersama OJK dan pihak terkait lain akan melakukan evaluasi menyeluruh untuk mencegah kejadian serupa di masa depan.[2]

Bobolnya data Bank Syariah Indonesia tidak hanya berdampak secara finansial dan reputasi bank, tetapi juga membuat nasabah menjadi rentan terhadap penipuan dan pencurian identitas. Kejadian ini merongrong kepercayaan masyarakat terhadap sistem perbankan syariah dan keamanan siber secara umum. Ini menyoroti tantangan dalam

keamanan siber yang perlu diatasi, termasuk perlindungan data pribadi dan keuangan, pembaruan sistem keamanan, dan peningkatan kesadaran terhadap keamanan siber.

Untuk mengatasi permasalahan ini, langkah-langkah konkret harus diambil. Bank dan lembaga keuangan harus meningkatkan infrastruktur keamanan mereka, melibatkan sistem proteksi data dan pemantauan keamanan yang efektif. Pelatihan dan kesadaran terkait keamanan siber harus diperkuat untuk melibatkan seluruh karyawan dan nasabah. Kerja sama antar lembaga keuangan, pemerintah, dan lembaga penegak hukum juga perlu ditingkatkan untuk melacak dan menghukum pelaku kejahatan siber.

Peristiwa bobolnya data Bank Syariah Indonesia menegaskan urgensi keamanan siber dalam melindungi sistem keuangan dan privasi pelanggan. Ancaman serius ini memerlukan perhatian serius dari berbagai pihak. Dengan langkah-langkah tepat, seperti peningkatan infrastruktur keamanan dan peningkatan kesadaran terhadap keamanan siber, diharapkan dapat menciptakan sistem keuangan yang aman, andal, dan sesuai dengan prinsip-prinsip syariah. Sehingga, masyarakat dapat memanfaatkannya dengan percaya diri dan nyaman.[3]

[1] Assiffa, B. A. (2023). PERLINDUNGAN HUKUM TERHADAP NASABAH BANK SYARIAH INDONESIA DARI SERANGAN CYBERCRIME (bachelorThesis). Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta

[2] Hosnah, A. U., Antoni, H., & Yofany, R. (2023). Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law. International Journal of Multicultural and Multireligious Understanding, 10(4), 362–372. Retrieved 6 November 2023 from https://doi.org/10.18415/ijmmu.v10i4.4643

[3] Tambunan, N., Wulandari, A. F., Pangesti, A. N., Anggraini, A., Tunnaja, S., Gita, A. D., & Rusmarhadi, I. (2023). BERITA UTAMA TENTANG ERROR SERVICE DI BANK SYARIAH INDONESIA (BSI). Community Development Journal : Jurnal Pengabdian Masyarakat, 4(2), 5096–5098.

Rumusan Masalah

1. Bagaimana aspek perlindungan hukum bagi konsumen PT. Bank Syariah Indonesia sesuai dengan ketentuan Undang-Undang Perlindungan Konsumen (UUPK)?

2. Apa bentuk tanggung jawab PT. Bank Syariah Indonesia terkait kebocoran data nasabahnya menurut Undang-Undang Perlindungan Konsumen (UUPK)?

Metode Penelitian

Penelitian ini mengambil pendekatan metode normatif sebagai dasar utama untuk menganalisis kasus yang sedang diuji. Dengan metode ini, peneliti dapat menghubungkan temuan mereka dengan teori-teori dan norma hukum yang ada dalam peraturan perundang-undangan yang relevan. Pendekatan ini memfasilitasi pemahaman konteks hukum yang mengatur kasus tersebut dan memungkinkan evaluasi apakah tindakan yang diambil sesuai dengan kerangka hukum yang berlaku.

Sumber data utama dalam penelitian ini adalah bahan hukum primer, terutama Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen. Bahan hukum primer memberikan dasar konkret untuk menganalisis dan mengevaluasi tindakan yang terkait dengan kasus ini. Dengan merinci ketentuan-ketentuan undang-undang tersebut, peneliti dapat menyusun argumen yang kuat berdasarkan landasan hukum yang jelas.

Selain itu, penelitian ini memanfaatkan bahan hukum sekunder sebagai pendukung analisis. Artikel, jurnal, dan buku yang relevan dengan topik ini digunakan sebagai sumber tambahan untuk mendukung dan memperdalam pemahaman isu hukum yang sedang diteliti. Bahan hukum sekunder membuka perspektif lebih luas dan memungkinkan peneliti melihat isu ini dari berbagai sudut pandang yang mungkin tidak tercakup dalam bahan hukum primer.

Dalam proses pengumpulan data, penelitian ini mengadopsi metodologi yang cermat dan sistematis. Identifikasi, pengumpulan, dan analisis data dilakukan dengan teliti untuk memastikan validitas dan reliabilitas tinggi.

Pendekatan interdisipliner juga diterapkan dalam penelitian ini dengan mempertimbangkan aspek-aspek hukum dan merangkum pandangan dari berbagai sumber. Hal ini bertujuan untuk memberikan gambaran yang lebih komprehensif terhadap kasus yang sedang dipelajari.

Dengan mengombinasikan metode normatif, bahan hukum primer, dan bahan hukum sekunder, diharapkan penelitian ini dapat memberikan kontribusi yang berharga dalam pemahaman dan penyelesaian kasus yang sedang dibahas.

Hasil dan Pembahasan

Pendekatan penelitian ini membuka cakrawala yang lebih luas terhadap upaya melindungi konsumen, khususnya dalam kasus pelanggaran keamanan data nasabah PT. Bank Syariah Indonesia. Melalui metode ini, kita dapat mendapatkan pemahaman yang lebih mendalam, mengungkap akar permasalahan, dan mengidentifikasi implikasi yang mungkin terlewat sebelumnya.

Dengan memperluas pemahaman terhadap dinamika insiden keamanan data, penelitian ini tidak hanya terbatas pada analisis kasus semata, melainkan juga memberikan sumbangan

berharga untuk pengembangan kebijakan. Informasi yang dikumpulkan dapat menjadi dasar yang kuat untuk merancang dan melaksanakan strategi

perlindungan yang lebih efektif. Oleh karena itu, hasil penelitian ini tidak hanya menawarkan solusi jangka pendek untuk kasus tertentu, tetapi juga membentuk dasar untuk perlindungan berkelanjutan terhadap masyarakat dari potensi kebocoran data nasabah di masa depan.

1. Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Berdasarkan UUPK.

Perlindungan konsumen memang menjadi dasar penting dalam menjaga kesejahteraan masyarakat. Namun, melihat kebocoran data di PT. Bank Syariah Indonesia, Undang-Undang (UU) No. 8 Tahun 1999 perlu diperbarui agar lebih responsif terhadap tantangan keamanan data di era digital.

Pasal 4 UUPK menyebut hak-hak konsumen yang seharusnya dilindungi oleh bank, termasuk hak atas kenyamanan, keamanan, dan keselamatan data nasabah. Namun, serangan siber oleh kelompok hacker LockBit menunjukkan bahwa standar keamanan bank mungkin tidak sesuai dengan risiko di dunia maya.

Peran pemerintah dan lembaga pengawas, seperti OJK, penting dalam menangani ini. Meskipun nasabah bisa mengajukan keluhan ke OJK, sistem pengawasan perlu ditingkatkan agar lembaga keuangan menerapkan praktik keamanan data yang memadai. Kerja sama pemerintah dan OJK dengan sektor swasta diperlukan untuk mengembangkan pedoman keamanan data yang ketat.[4]

Regulasi fintech juga harus diperbarui untuk mengakomodasi ancaman keamanan siber. Keamanan data harus menjadi fokus utama, dan sanksi yang tegas harus diberlakukan untuk mencegah kelalaian penyedia layanan keuangan. Kerjasama antara regulator dan sektor swasta dalam menyusun kebijakan yang efektif sangat penting.

Transparansi pemerintah tentang kebocoran data dan langkah-langkah yang diambil penting untuk membangun kembali kepercayaan masyarakat. Komunikasi jelas mengenai tindakan perbaikan oleh Bank Syariah Indonesia dan tindak lanjut pemerintah dapat mengurangi kekhawatiran nasabah.

Kasus ini mencerminkan pelanggaran terhadap prinsip keamanan data, privasi, dan etika. Selain kerugian materiil, ini merusak kredibilitas Bank Syariah Indonesia. Oleh karena itu, perusahaan perlu fokus pada perbaikan sistem keamanan data dan memastikan pengamanan data menjadi prioritas.[5]

Tanggapan holistik dan berkelanjutan diperlukan. Perbaikan sistem keamanan data harus menjadi prioritas, dengan teknologi terbaru dan ahli keamanan siber. Peningkatan transparansi melalui pelaporan rutin dapat membangun kembali kepercayaan.

[4] Ilhami, D. A. S. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi, 2(1).
[5] Norrahman, R. A. (2023). Peran Fintech Dalam Transformasi Sektor Keuangan Syariah. JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, Dan Akuntansi, 1(2), 101–126.

Sanksi tegas terhadap kelalaian keamanan data perlu ditegakkan, termasuk sanksi finansial dan hukum. Ini memberikan efek jera dan mendorong perusahaan menghadapi tanggung jawab keamanan data.

Edukasi masyarakat tentang pentingnya keamanan data tidak boleh diabaikan. Pemahaman nasabah tentang melindungi informasi pribadi dan mengidentifikasi ancaman siber dapat menciptakan lingkungan tanggung jawab bersama antara perusahaan dan konsumen.

Dengan mengambil langkah-langkah ini, kita dapat memastikan perlindungan nasabah dan kepercayaan masyarakat pada sistem keuangan tetap terjaga. Ini juga mendorong perusahaan keuangan meningkatkan praktik keamanan data demi keberlanjutan dan kesejahteraan bersama.

2. Bentuk Pertanggung jawaban PT. Bank Syariah Indonesia

PT. Bank Syariah Indonesia (BSI) sebagai subjek usaha bertanggung jawab untuk memberikan kompensasi terhadap kerugian, pencemaran, dan/atau kerugian yang dialami konsumen akibat konsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan. Ini sesuai dengan Pasal 19 ayat (1), (2), (3), dan (4) Undang-Undang Perlindungan Konsumen (UUPK), yang mengamanatkan bank untuk mengganti kerugian nasabah yang muncul karena gangguan sistem yang menghambat transaksi.

Ganti rugi ini dapat berupa pengembalian uang atau penggantian barang dan/atau jasa setara. Meskipun demikian, perlu diingat bahwa memberikan ganti rugi tidak menghapuskan kemungkinan tuntutan pidana, tergantung pada bukti lebih lanjut terkait kesalahan. Selain itu, jika pelaku usaha dapat membuktikan bahwa kesalahan tersebut merupakan kesalahan konsumen, ketentuan ganti rugi tidak berlaku.

Dalam konteks insiden peretasan data yang diduga terjadi pada PT. Bank Syariah Indonesia oleh kelompok hacker LockBit, yang mengakibatkan gangguan transaksi keuangan nasabah, perlu diinvestigasi dengan hati-hati. Jika terbukti bahwa kebocoran data disebabkan oleh kelalaian bank, nasabah berhak mendapatkan ganti rugi. Namun,

jika kesalahan dapat dibuktikan sebagai kesalahan konsumen, bank tidak berkewajiban memberikan ganti rugi.

Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) dapat menjadi landasan hukum untuk menilai apakah tindakan PT. Bank Syariah Indonesia dianggap perbuatan melawan hukum. Pasal ini menegaskan bahwa setiap perbuatan yang melanggar hukum dan merugikan orang lain wajib mengganti kerugian yang timbul.

Penting untuk dicatat bahwa ganti rugi harus mencakup pengembalian data yang bocor akibat kelalaian PT. Bank Syariah Indonesia. Dalam konteks ini, nasabah berhak untuk menuntut ganti rugi melalui pengadilan negeri yang memiliki kompetensi absolut dan kompetensi relatif sesuai dengan Pasal 113 Hukum Acara Perdata.

Dalam proses hukum ini, beban pembuktian terletak pada pihak penggugat, yaitu nasabah yang mengalami masalah akibat kebocoran data. Mereka perlu menyajikan bukti yang kuat untuk menunjukkan bahwa bank bertanggung jawab atas kebocoran data dan merugikan mereka secara finansial maupun operasional.

Penting untuk diingat bahwa nasabah dan PT. Bank Syariah Indonesia mungkin mencapai penyelesaian di luar pengadilan melalui mediasi atau negosiasi. Namun, jika

penyelesaian damai tidak tercapai, pengadilan akan menjadi forum untuk menilai dan memutuskan tuntutan ganti rugi nasabah.

Dalam menetapkan tuntutan ganti rugi, nasabah harus dengan cermat menghitung kerugian yang mereka alami akibat kebocoran data, termasuk potensi kerugian finansial, reputasi, dan dampak operasional. Semakin lengkap dan kuat bukti yang dimiliki, semakin besar kemungkinan mereka untuk mendapatkan ganti rugi yang diinginkan.

Untuk memastikan transparansi dan keadilan, pengadilan perlu mengadakan sidang dengan mempertimbangkan argumen dari kedua belah pihak. Dalam hal ini, keberlakuan hukum dan norma-norma dalam UUPK dan KUHPerdata akan menjadi panduan utama dalam pengambilan keputusan.

Selain itu, perlu dieksplorasi apakah ada langkah-langkah yang dapat diambil untuk memperkuat keamanan data di masa depan, agar kasus serupa tidak terulang. Ini dapat melibatkan peningkatan keamanan teknologi informasi, pelatihan karyawan, dan implementasi kebijakan keamanan data yang lebih ketat.

Dengan demikian, kasus PT. Bank Syariah Indonesia terhadap nasabahnya yang diduga melibatkan peretasan data dapat menjadi pengajaran berharga bagi sektor perbankan dan industri secara keseluruhan untuk meningkatkan keamanan data dan melindungi kepentingan nasabah.[6]

3. Manajemen risiko dalam operasional PT. Bank Syariah Indonesia menitikberatkan pada peningkatan aspek keamanan dan kesinambungan bisnis.

Manajemen risiko operasional di PT. Bank Syariah Indonesia (BSI) menitikberatkan pada peningkatan aspek keamanan dan kontinuitas bisnis sebagai bagian tak terpisahkan dari upaya menjaga kinerja, reputasi, dan kelangsungan usaha bank. Dalam menghadapi risiko operasional, BSI telah mengambil langkah-langkah strategis untuk memastikan setiap aspek kegiatan operasional dikelola dengan efektif dan efisien.

Langkah awal yang diambil oleh BSI adalah menyusun kebijakan, prosedur, dan pedoman manajemen risiko operasional yang berlaku di seluruh unit kerja dan jaringan kantor, termasuk di wilayah Aceh. Kebijakan ini tidak hanya didasarkan pada prinsip- prinsip syariah, tetapi juga mencakup dasar hukum, peraturan yang relevan, dan standar internasional yang diakui secara umum. Dengan demikian, BSI memastikan setiap tindakan selaras dengan kerangka kerja yang berlaku dan mendukung keberlanjutan bisnis syariah.[7]

Identifikasi, pengukuran, pemantauan, dan pengendalian risiko operasional merupakan aspek kritis dalam manajemen risiko. BSI menjalankan proses ini secara berkelanjutan dan komprehensif dengan menggunakan metode dan alat yang sesuai, seperti self-assessment, key risk indicators, loss event database, risk and control matrix, dan lainnya. Pendekatan ini memungkinkan bank untuk secara proaktif mengidentifikasi dan mengelola risiko operasional yang mungkin muncul, sehingga dapat mengurangi potensi dampak negatifnya.

Teknologi Informasi (TI) yang aman dan handal dalam operasional perbankan syariah menjadi sangat penting. Oleh karena itu, BSI telah mengadopsi penggunaan TI yang memenuhi standar keamanan data, backup dan recovery, business continuity plan, disaster recovery plan,

[6] Isnaini, A. M. (2022). Pertanggungjawaban Dewan Pengawas Syariah (DPS) Dalam Operasional Perbankan Syariah. Jatiswara, 37(3).

[7] Azis, A., Mulyana, R., & Fauzi, R. (2023). Penyusunan Manajemen Risiko TI Berdasarkan Cobit 2019 I&T Risk Focus Area Untuk Digitalisasi Fintechco. J-SAKTI (Jurnal Sains Komputer Dan Informatika), 7(2), 940-956.

dan aspek-aspek lainnya. Dengan berinvestasi dalam teknologi, bank dapat meningkatkan efisiensi operasional sambil tetap menjaga keamanan dan ketersediaan data.

Sebagai langkah konkret untuk memastikan keamanan, BSI juga menerapkan program anti pencucian uang dan pendanaan terorisme (APU-PPT) sesuai dengan ketentuan syariah dan peraturan yang berlaku. Program ini dirancang untuk mencegah dan mendeteksi aktivitas mencurigakan atau ilegal yang dapat merugikan bank atau nasabah. Dengan demikian, BSI berkomitmen untuk beroperasi sesuai dengan nilai-nilai syariah dan integritas bisnis.[8]

Selain fokus pada keamanan, BSI menitikberatkan pada kesinambungan bisnis. Bank ini mengembangkan sistem informasi manajemen risiko operasional yang terintegrasi dan dapat diandalkan. Sistem ini mendukung proses pengambilan keputusan, pelaporan, dan komunikasi yang efektif dan tepat waktu. Dengan adanya sistem ini, BSI dapat dengan cepat merespons gangguan atau bencana yang mungkin terjadi, meminimalkan dampaknya, dan memulihkan fungsi-fungsi kritis secara efisien.

Pengembangan sumber daya manusia (SDM) juga menjadi bagian tak terpisahkan dari manajemen risiko operasional BSI. Bank ini memberikan perhatian khusus pada pelatihan dan pengembangan SDM yang berkualitas, profesional, dan berintegritas. Dengan meningkatkan kompetensi, kinerja, dan tanggung jawab SDM, BSI dapat memastikan bahwa setiap individu di dalam organisasi memiliki pemahaman yang baik terhadap risiko operasional dan dapat berkontribusi secara maksimal dalam mengelolanya.

Koordinasi dan kerjasama dengan pihak-pihak internal dan eksternal menjadi landasan penting dalam manajemen risiko operasional BSI. Dengan berkolaborasi dengan Dewan Pengawas Syariah, Dewan Komisaris, auditor internal dan eksternal, regulator, asosiasi, dan pihak lainnya, BSI dapat memastikan bahwa setiap tindakan selaras dengan standar industri dan peraturan yang berlaku.

Dengan menerapkan langkah-langkah ini, BSI berharap dapat meningkatkan aspek keamanan dan kesinambungan bisnis dalam manajemen risiko operasionalnya. Lebih dari sekadar kepatuhan terhadap regulasi, bank ini berupaya memberikan nilai tambah bagi pemangku kepentingan, meningkatkan kepercayaan masyarakat, dan mendukung pertumbuhan ekonomi syariah di Indonesia. Melalui pendekatan holistik ini, BSI membuktikan komitmennya untuk menjaga integritas dan kinerja yang berkesinambungan dalam menghadapi dinamika risiko operasional di industri perbankan syariah.

[8] Prabantarikso, D. R. M., M.M, E. F., S. E., Ph.D, Z. A., & Abdulrachman, D. Y. (2022). Konsep Dan Penerapan Manajemen Risiko Operasional: RCSA-KRI-LED. Deepublish.

Kesimpulan

Secara esensial, perlindungan konsumen terhadap nasabah PT. Bank Syariah Indonesia (BSI) berdasarkan Undang-Undang Perlindungan Konsumen (UUPK) memerlukan penyegaran agar lebih tanggap terhadap tantangan keamanan data di era digital. Meskipun UUPK menetapkan hak-hak konsumen, serangan siber oleh kelompok hacker LockBit di BSI menunjukkan bahwa standar keamanan bank mungkin kurang memadai.

Pentingnya peran pemerintah dan lembaga pengawas, seperti OJK, menjadi fokus dalam menangani kebocoran data. Diperlukan peningkatan sistem pengawasan agar lembaga keuangan menerapkan praktik keamanan data yang memadai. Kerja sama antara pemerintah, OJK, dan sektor swasta perlu ditingkatkan untuk mengembangkan pedoman keamanan data yang ketat.

Regulasi fintech juga perlu diperbarui untuk mengantisipasi ancaman keamanan siber, terutama pada aspek keamanan data, dan memberlakukan sanksi yang tegas untuk mencegah kelalaian penyedia layanan keuangan. Keterbukaan pemerintah dalam menangani kebocoran data dan langkah-langkah yang diambil menjadi kunci untuk memulihkan kepercayaan masyarakat.

Kejadian kebocoran data di BSI mencerminkan pelanggaran terhadap prinsip keamanan data, privasi, dan etika, yang merugikan tidak hanya secara materiil tetapi juga merusak kredibilitas bank. Oleh karena itu, perusahaan perlu fokus pada perbaikan sistem keamanan data dan memastikan bahwa perlindungan data menjadi prioritas.

Respon yang holistik dan berkelanjutan diperlukan, dengan perbaikan sistem keamanan data sebagai fokus utama. Peningkatan keterbukaan melalui pelaporan rutin dapat membantu membangun kembali kepercayaan masyarakat. Sanksi yang tegas terhadap kelalaian keamanan data harus ditegakkan, termasuk sanksi finansial dan hukum untuk mencegah kejadian serupa di masa depan.

Pendidikan masyarakat mengenai pentingnya keamanan data tidak boleh diabaikan. Pemahaman nasabah mengenai perlindungan informasi pribadi dan identifikasi ancaman siber dapat menciptakan lingkungan tanggung jawab bersama antara perusahaan dan konsumen.

Dalam konteks pertanggungjawaban BSI terhadap nasabahnya, UUPK memberikan dasar hukum untuk memberikan kompensasi terhadap kerugian yang diderita konsumen akibat gangguan sistem. Namun, perlu dipastikan bahwa ganti rugi mencakup pengembalian data yang bocor dan bahwa proses hukum berlangsung adil dan transparan.

Manajemen risiko operasional BSI menunjukkan fokus pada keamanan dan kelangsungan bisnis. Dengan langkah-langkah strategis, penggunaan teknologi informasi yang aman, pengembangan sumber daya manusia, dan kerjasama dengan pihak eksternal, BSI berkomitmen untuk mengelola risiko operasional secara efektif.

Secara keseluruhan, penyempurnaan regulasi, peningkatan keterbukaan, sanksi yang tegas, edukasi masyarakat, dan penekanan pada keamanan dan kelangsungan bisnis menjadi faktor kunci untuk memastikan perlindungan nasabah, memulihkan kepercayaan masyarakat, dan meningkatkan integritas industri perbankan syariah di Indonesia.

Saran

Dalam menghadapi tantangan keamanan data dan perlindungan konsumen di PT. Bank Syariah Indonesia (BSI), beberapa rekomendasi dapat diajukan untuk meningkatkan keamanan dan memperbarui kepercayaan masyarakat.

1. diperlukan pembaruan regulasi, terutama Undang-Undang Perlindungan Konsumen (UUPK) dan regulasi fintech, agar lebih responsif terhadap ancaman keamanan siber di era digital. Regulasi ini perlu mencakup standar keamanan data yang lebih ketat dan sanksi yang tegas untuk mendorong perusahaan keuangan menjaga keamanan informasi nasabah.

2. perlu ditingkatkan sistem pengawasan oleh lembaga seperti OJK untuk memastikan bahwa bank dan lembaga keuangan lainnya menerapkan praktik keamanan data yang memadai. Kerjasama antara pemerintah, lembaga pengawas, dan sektor swasta dalam menyusun pedoman keamanan data yang efektif juga sangat penting.

3. Bank Syariah Indonesia harus menekankan perbaikan sistem keamanan data dan memastikan investasi dalam teknologi terbaru dan keahlian keamanan siber. Penerapan teknologi yang memenuhi standar keamanan data, pelatihan karyawan, dan implementasi kebijakan keamanan data yang ketat harus menjadi fokus utama.

4. transparansi pemerintah dan BSI tentang kebocoran data serta langkah-langkah yang diambil perlu ditingkatkan. Komunikasi yang jelas dan terbuka mengenai tindakan perbaikan oleh bank dan respons pemerintah dapat membantu mengurangi kekhawatiran nasabah dan membangun kembali kepercayaan.

5. edukasi masyarakat tentang pentingnya keamanan data dan cara melindungi informasi pribadi mereka perlu ditingkatkan. Program edukasi yang ditargetkan kepada nasabah dan masyarakat umum dapat menciptakan kesadaran akan ancaman siber dan meningkatkan tanggung jawab bersama dalam menjaga keamanan data.

6. dalam konteks pertanggungjawaban BSI terhadap nasabahnya, perlu ditegakkan proses hukum yang adil dan transparan. Selain itu, bank harus secara proaktif memberikan kompensasi yang memadai kepada nasabah yang mengalami kerugian akibat kebocoran data.

Dengan menerapkan rekomendasi ini, diharapkan BSI dapat memperkuat keamanan data, membangun kembali kepercayaan masyarakat, dan meningkatkan integritas industri perbankan syariah secara keseluruhan.

Referensi

Peraturan Perundang-Undangan

Pasal 113 Hukum Acara Perdata

Pasal 1365 Kitab Undang-Undang Hukum Perdata

Pasal 19 ayat (1), (2), (3), dan (4) Undang-Undang Perlindungan Konsumen Pasal 4 UUPK tentang hak-hak konsumen

Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen

Buku

Prabantarikso, D. R. M., M.M, E. F., S. E., Ph.D, Z. A., & Abdulrachman, D. Y. (2022). Konsep Dan Penerapan Manajemen Risiko Operasional: RCSA-KRI-LED. Deepublish.

Lain-lain

Assiffa, B. A. (2023). PERLINDUNGAN HUKUM TERHADAP NASABAH BANK SYARIAH

INDONESIA DARI SERANGAN CYBERCRIME (bachelorThesis). Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta. Retrieved 9 November 2023 from https://repository.uinjkt.ac.id/dspace/handle/123456789/74011

Azis, A., Mulyana, R., & Fauzi, R. (2023). Penyusunan Manajemen Risiko TI Berdasarkan Cobit 2019 I&T Risk Focus Area Untuk Digitalisasi Fintechco. J-SAKTI (Jurnal Sains Komputer Dan Informatika), 7(2), 940–956. Retrieved 9 November 2023 from https://doi.org/10.30645/j-sakti.v7i2.698

Hosnah, A. U., Antoni, H., & Yofany, R. (2023). Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law. International Journal of Multicultural and Multireligious Understanding, 10(4), 362–372. Retrieved 6 November 2023 from https://doi.org/10.18415/ijmmu.v10i4.4643

Ilhami, D. A. S. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi, 2(1). Retrieved 9 November 2023 from https://doi.org/10.20885/snati.v2i1.19

Isnaini, A. M. (2022). Pertanggungjawaban Dewan Pengawas Syariah (DPS) Dalam Operasional Perbankan Syariah. Jatiswara, 37(3). Retrieved 9 November 2023 from https://doi.org/10.29303/jtsw.v37i3.428