Jurnal Perbankan Syariah Darussalam (JPSDa)
Vol.5 / No.1: 26-40, Januari 2025,
ISSN : 2775-6084 *(online)*
Doi : 10.30739/jpsda.v5i1.3581
Terakreditasi Sinta 5: No 72/E/KPT/2024

Submit: 27-12-2024
Editor: 30-12-2024
Reviewed:18-01-2025
Publish: 24-01-2025

STRATEGI PENGUATAN DATABASE NASABAH PADA PERBANKAN SYARIAH

Tri Ibnu Ramadhanu[1], Syahrul Tanjung[2], Heri Yunus[3], Habibul Ahir[4], Nurbaiti [5]
Universitas Islam Negeri Sumatera Utara[1,2,3,4,5]
triiburamadhanu@gmail.com[1], syahrultanjungpku@gmail.com[2], lubish159@gmail.com[3], habibulahir@gmail.com[4], nurbaiti@uinsu.ac.id[5]

Abstrak

Potensi serangan siber sektor keuangan, khususnya perbankan, adalah yang paling rentan terhadap serangan siber. Serangan yang paling umum termasuk phishing dan ransomware yang dialamai PT. Bank Syariah Indonesia pada mei 2023, sebanyak 15 juta data milik nasabah dan karyawan PT. Bank Syariah Indonesia telah dicuri oleh kelompok peretas ransomware lockbit 3.0. Tujuan penelitian ini adalah memberikan konsep strategi penguatan database nasabah pada perbankan syariah yang dapat menjadi rujukan pihak perbankan syariah kedepannya dalam mengatasi serangan siber. Penelitian ini menggunakan metode kualitatif pendekatan deskriptif. Penelitian ini menghasilakan 3 strategi dalam menguatkan database nasabah bank syariah: Pencadangan data (back up data), Arsitektur teknologi perbankan, serta regulasi pemerintah. Dengan adanya database yang kuat maka amanah yang dipertanggungjawabkan oleh perbankan syariah dapat terlaksana. Penulis menyarankan kepada pihak pemerintah untuk merumuskan undang-undang secara khusus yang mengatur mengenai internet banking guna menjaga keamananan database perbankan syariah.

Kata Kunci: Manajemen Strategi, Database, Keamanan sistem perbankan.

Abstract

Potential cyber attacks the financial sector, particularly banking, is the most vulnerable to such threats. The most common attacks include phishing and ransomware, as experienced by PT. Bank Syariah Indonesia in May 2023, where 15 million pieces of data belonging to customers and employees were stolen by the Lockbit 3.0 ransomware hacking group. The aim of this study is to provide a strategy concept for strengthening customer databases in Islamic banking, which can serve as a reference for Islamic banking institutions in the future to address cyberattacks. This research employs a qualitative method with a descriptive approach. The study identifies three strategies for enhancing customer databases in Islamic banks: Data backup, Banking technology architecture, and Government regulations. With a strong database in place, the trust entrusted to Islamic banks can be upheld. The author

recommends that the government formulate specific legislation regulating internet banking to safeguard the security of the Sharia Banking databases.

Keywords: Strategic Manajemen, Database, Banking System Security

A. PENDAHULUAN

Pada tahun 1992, Indonesia mencatat sejarah penting dengan didirikannya Bank Muamalat Indonesia sebagai bank syariah pertama. Bank ini didirikan oleh pemerintah Indonesia dan Majelis Ulama Indonesia (MUI), sebuah lembaga penting dalam penentuan kesesuaian produk dan layanan dengan prinsip-prinsip syariah (Fahrurrozie 2023) Bank Muamalat Indonesia merupakan lembaga perbankan syariah pertama dan pionir bank syariah lainnya secara bertahap menerapkan sistem ini. Selama krisis keuangan tahun 1998, bank-bank konvensional bangkrut, sementara bank-bank yang menerapkan sistem syariah tetap stabil.

Perbankan syariah dalam menjalankan operasionalnya memerlukan penyimpanan sistem informasi berupa database yang aman. Keamanan database merupakan suatu hal yang krusial untuk menjamin bahwa data yang tersimpan dalam sistem tetap aman dan dapat diakses dengan lancar. Proses ini melibatkan berbagai langkah untuk menjamin bahwa data hanya dapat diakses oleh pihak tertentu yang berhak, dan tidak bisa dijangkau oleh pihak yang tidak memiliki otoritas. Keamanan database mencakup beberapa elemen, seperti kebijakan pengamanan, pengelolaan hak akses, enkripsi data, pemulihan dan cadangan data, serta pemantauan dan pengawasan secara terus-menerus.

Kebijakan keamanan database merujuk pada seperangkat pedoman dan peraturan yang dibuat untuk menjaga agar data tetap aman dan terhindar dari penyalahgunaan. Sementara itu, manajemen akses berfokus pada pengaturan izin atau hak akses bagi pengguna database. Dengan demikian, hanya pihak berwenang yang memiliki akses terhadap data yang tersedia. Enkripsi data adalah teknik untuk mengubah informasi menjadi format yang tidak bisa dibaca tanpa kunci dekripsi yang tepat. Proses backup dan recovery mencakup pembuatan salinan cadangan data serta pemulihan data yang hilang atau rusak. Terakhir, pengawasan dan monitoring dilakukan untuk memantau dan merekam setiap interaksi dengan database guna mendeteksi kemungkinan ancaman terhadap keamanan. (Ujung, Irwan, dan Nasution 2023).

Pemantauan dan pengawasan yang kontinu adalah langkah krusial dalam menerapkan sistem keamanan yang efektif pada database nasabah. Perbankan syariah harus mempunyai metode pegawasan yang berkelanjutan untuk mengidentifikasi potensi serangan atau aktivitas diluar nalar dalam *network* mereka. Penerapan kontrol keamanan yang tepat dan kepatuhan terhadap standar yang berlaku sangat penting

untuk mempertahankan nama baik bank syariah serta menunaikan ekspektasi konsumen terkait dengan isolasi dan perlindungan data (Faizal et al. 2023).

Bank syariah memiliki kerentanan terhadap serangan phishing, yang memanfaatkan psikologis untuk mendapatkan informasi pribadi dari nasabah atau karyawan . Phishing adalah teknik peretasan di mana pelaku berusaha mengakses data sensitif contohnya meliputi data seperti nama, alamat, dan usia. Serangan ini umumnya dilakukan dengan mengirimkan pesan palsu melalui email, surat, atau saluran komunikasi lainnya. Pelaku kejahatan siber kerap menyamar sebagai lembaga tepercaya, seperti bank, instansi pemerintah, atau platform digital, dengan tujuan menipu korban. Pesan tersebut biasanya berisi permintaan agar korban mengungkapkan informasi pribadi atau mengakses tautan yang mengarahkan ke situs web tiruan yang dirancang untuk mencuri data tersebut. (Ramadhanti Achlina Tri Putri dan Heru Sugiyono 2024).

Keberhasilan serangan phishing dapat mencoreng reputasi bank syariah dan menyebabkan kerugian finansial bagi nasabah. Selain itu, ancaman dari malware atau ransomware bisa dapat menyebabkan kebocoran data, pencurian informasi keuangan, atau penguncian sistem yang mengganggu kelancaran operasional bank. Selain itu, dapat mengakibatkan kehilangan kendali atas sistem dan data sensitif, serta meningkatkan risiko pembayaran tebusan dalam kasus serangan ransomware. (Restika dan Sonita 2023) Ransomware atau malware dapat menginfeksi komputer melalui berbagai metode, seperti melalui file lampiran yang diunduh oleh korban, atau menyerang langsung perangkat lunak dengan mencari celah yang rentan. (Nurul Monika Larasati dan Rayyan Firdaus 2024).

Potensi serangan siber sektor keuangan, khususnya perbankan, adalah yang paling rentan terhadap serangan siber, dikutip dari BSSN (Badan Siber dan Sandi Negara). Serangan yang paling umum termasuk phishing dan ransomware. Oleh karena itu, bank harus mempertahankan keamanan siber secara konsisten untuk meningkatkan resistensi mereka terhadap berbagai pola serangan siber baru. Beberapa upaya yang dapat dilakukan oleh bank antara lain dengan melakukan pengujian keamanan siber, menilai kemampuan keamanan siber secara mandiri, dan melaporkan insiden siber. Selain itu, peningkatan teknologi menyebabkan peningkatan penggunaan pihak ketiga yang dapat menimbulkan potensi risiko tambahan, sepertirisiko operasional. Selain itu, kemajuan teknologi harus diimbangi oleh kesiapan organisasi, termasuk pemimpin dan talenta digital yang cukup, baik secara kuantitas maupun kualitas, Budaya organisasi yang berfokus pada digitalisasi dan struktur organisasi yang mendukung transformasi digital. (Satrya Ilham Zharfan 2024).

Pada Pada 8 Mei 2023, Bank Syariah Indonesia menghadapi serangan siber di mana peretas ransomware Lockbit 3.0 berhasil mencuri data sebanyak 15 juta nasabah dan pegawai. Kelompok peretas tersebut mengklaim telah mengakses dan merusak

sistem Bank Syariah Indonesia, menyebabkan seluruh layanan bank terhenti. Para pelaku tersebut mengaku mencuri sekitar 1,5 terabyte data yang mencakup informasi pribadi seperti nama, alamat, nomor kartu, nomor telepon, serta transaksi nasabah dan lembaga. Selain itu, mereka juga mengklaim telah mencuri dokumen keuangan, dokumen hukum, serta kata sandi untuk seluruh layanan internal dan eksternal yang digunakan oleh bank. (Intan 2023).

Menurut yang dikemukakan oleh dewi, dkk. Bahwa penyebab terjadinya peretasan database nasabah di Bank Syariah Indonesia yang terjadi pada 8 mei 2023 adalah disebabkan oleh *maintenance system* (sistem pemeliharaan) dan indikasi adanya serangan siber. (Fatmala Putri dan Ratna Sari 2023). Kerugiannya yaitu seperti yang dikutip dari situs CNN Indonesia berdasarkan hasil wawancara pihak CNN Indonesia dengan Corporate Secretary BSI Gunawan Arif Hartoyo, bahwa sekitar 1200 unit ATM BSI dan kantor-kantor BSI mengalami gangguan (CNN Indonesia 2023). Adapun solusinya akibat serangan siber tersebut menurut Bagus dan Nasrulloh. Yaitu antara lain: *pertama.* Respons Cepat dan Tepat, *Kedua.* Peningkatan Teknologi Keamanan, *Ketiga.* Penawaran Insentif kepada Nasabah, dan *Keempat. s*penilaian dari internal dan ekternal Bank Syariah Indonesia. (Maulana dan Nasrulloh 2024).

Dengan melihat permasalahan diatas. Maka, penelitian ini selanjutnya merumuskan pertanyaan bagaimana penerapan strategi penguatan database nasabah pada perbankan syariah. Dengan tujuan untuk menghasilkan strategi penguatan database nasabah pada perbankan syariah. Dengan begitu penelitian ini menghasilkan kajian yang berbeda dari sebelumnya karena membahas strategi penguatan database nasabah pada perbankan syariah.

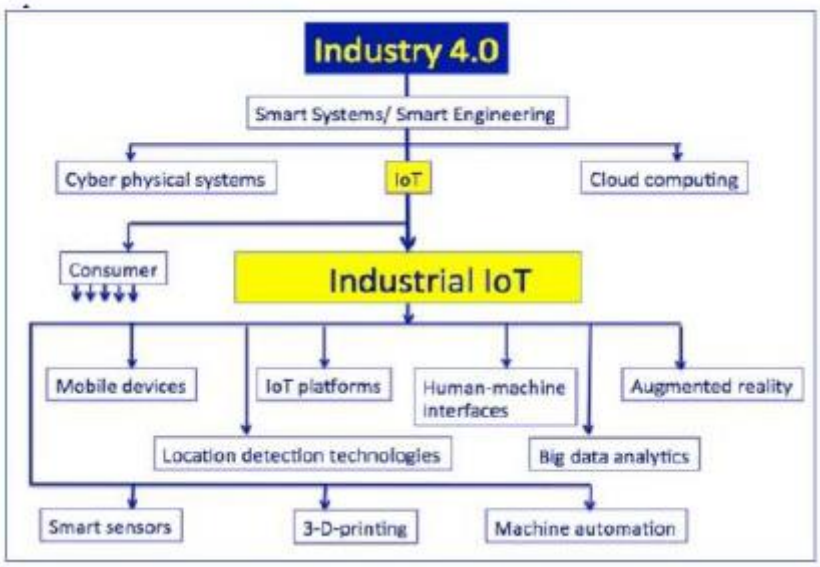
B. LANDASAN TEORI

1. Manajemen Strategi

Manajemen strategi dalam menjaga keamanan siber adalah sealur kegiatan, kebijakan, serta cara-cara yang disusun untuk menjaga system computer, jaringan, perangkat lunak, dan informasi (data) dari serangan peretasan serta ancaman keamanan lainnya. Strategi ini memiliki sifat komprehensif dan mencakup beberapa pendekatan untuk membendung ancaman dan peka terhadap potensi serangan siber. Beberapa strategi yang umum digunakan meliputi pengenalan ancaman (*threat intelligence*) untuk mengumpulkan informasi tentang potensi ancaman dunia maya, pelatihan dan kesadaran pengguna tentang praktik keamanan terbaik, pengembangan kebijakan keamanan yang jelas dan ketat, pemantauan dan deteksi dini menggunakan alat-alat yang tepat, pembaharuan perangkat lunak secara berkala, enkripsi data untuk melindungi informasi sensitive, manajemen akses dengan prinsip hak istimewa paling rendah, pencadangan data secara teratur, kolaborasi dan kemitraan dengan lembaga keamanan siber lainnya untuk berbagi intelijen ancaman siber. Dengan menerapkan

strategi kemanan siber yang holistic dan proaktif, perusahaan dapat mengurangi risiko serangan siber dan meminimalkan dampak serangan yang terjadi.

Manajemen strategi dalam menjaga database dari serangan siber yang digagas oleh Ade Irawan, dkk adalah dengan menerapkan konsep berbasis IoT (*Internet of Things*).



Gambar 1. Manajemen cyber berbasis IoT

Ekosistem IoT meningkatkan permukaan serangan siber, sehingga membutuhkan integrasi keamanan yang komprehensif di seluruh perangkat keras, perangkat lunak, protocol komunikasi, interkoneksi cloud, dan manajemen siklus hidup. Pengembang harus merekayasa control akses yang ketat, enkripsi data, deteksi anomaly, dan saluran pembaruan firmware, sementara tim hukum mengadvokasi kebijakan dan peraturan untuk mengurangi prevalensi kerentanan. Kolaborasi lintas departemen meningkatkan kesadaran situasional dan memastikan langkah-langkah keamanan tertanam dan harus diperkuat diseluruh jajaran teknologi IoT untuk memerangi risiko. Ekosistem tersebut keseluruhannya bergantung pada elemen manusia yang pada siklusnya tetap menjadi sumber kerentanan yang signifikan. Untuk menghadapi hal ini, institusi harus menerapkan rencana kerja edukasi ke masyarakat secara komprehensif untuk mencegah risiko serangan siber.

Teknologi dan inovasi IoT ini sangat penting dalam mengatasi beragam serangan siber kontemporer seperti *phishing, ransomware, malware,* dan penipuan lainnya berbasis internet. Meskipun, biaya masih menjadi hambatan dalam pengimplementasiannya (Ade Irawan et al. 2024).

2. Database

Database merupakan tempat penyimpanan data yang permanen di perangkat penyimpanan dan diambil oleh sistem informasi. Data akun pelanggan diambil saat bank memulai operasi harian, dan data akun yang diperbarui disimpan kembali ke database pada akhir hari. Penyimpanan permanen dapat terjadi di perangkat keras seperti hard disk komputer atau di pusat data di cloud. Data disimpan dalam bentuk ter struktur yang disebut basis data. Basis data dapat berupa tabel dimensi, di mana kolom mewakili atribut tabel dan baris merekam data tabel (terlihat struktur tabel di gambar, di mana kolom mewakili atribut tabel dan baris yang direkam data tabel).

Pandangan Laudon dan Laudon (2016) mengutarakan bahwa basis data terdiri dari kumpulan tabel dimensi yang saling terkait. Setiap tabel dalam basis data mewakili entitas bisnis seperti wira niaga, departemen, produk, atau karyawan. Basis data digunakan sebagai sumber daya perusahaan untuk memastikan ketersediaan data dalam sistem informasi. Pada awalnya, sistem informasi bisnis menggunakan sistem file untuk menyimpan, mengambil, dan manipulasi data. Banyak aplikasi bisnis pada era 19601970, dan awal 1980 diimplementasikan menggunakan bahasa pemrograman COBOL (Common Business-Oriented Language). Sistem file digunakan untuk. menyimpan dan menyediakan data untuk sistem informasi tertentu, seperti file data penjualan untuk sistem informasi penjualan atau file data akuntansi untuk sistem informasi akuntansi.

Kelemahan dari sistem file adalah penyebaran yang sama di banyak lokasi berbeda. Data yang sama muncul di banyak file berbeda atau di banyak bidang dalam file. Misalnya, nomor telepon muncul di sistem file penjualan dan juga di sistem file. kemungkinan membuat inkonsistensi data penting. Efek negatif dari memiliki data yang sama disimpan dalam bidang file akan berlipat ganda (dikenal sebagai redundansi data). Menghindari redundansi data dan memastikan konsistensi data sangat penting untuk menjaga integritas dan keandalan basis data. Penggunaan basis data yang terstruktur dengan baik dan normalisasi yang tepat dapat membantu mengurangi risiko redundansi data dan efek negatif yang mungkin timbul. (Restika dan Sonita 2023)

3. Keamanan Sistem Perbankan

Berikut adalah tahapan yang dapat dilakukan oleh pihak bank untuk meningkatkan keamanan sistem:

a. Sistem Kriptografi: Sistem ini memanfaatkan angka-angka yang disebut kunci (key) untuk mengamankan data. Kriptografi, yang juga dikenal sebagai sistem enkripsi, memiliki dua jenis utama, yaitu kriptografi simetris dan asimetris.
b. Firewall, Firewall merupakan sistem yang dirancang untuk melindungi jaringan dengan mencegah akses tidak sah ke area yang dilindungi dalam infrastruktur perusahaan. Sistem ini berfungsi untuk menghalangi pihak-pihak

yang mencoba mengakses jaringan tanpa izin dengan meningkatkan dan memperumit hambatan-hambatan yang ada (Maya Safitri, Sefri Larasati, dan Rizki Hari 2020).

C. METODE PENELITIAN

Dalam penelitian ini, penulis menerapkan pendekatan kualitatif deskriptif. Penelitian deskriptif kualitatif bertujuan untuk menggambarkan atau memotret secara menyeluruh dan mendalam situasi sosial yang sedang diteliti. Menurut Bogdan dan Taylor, sebagaimana dikutip oleh Lexy J. Moleong, pendekatan kualitatif adalah suatu metode penelitian yang menghasilkan data deskriptif dalam bentuk kata-kata tertulis atau lisan dari individu serta perilaku yang diamati (Lexy, J. M. 2007). Penelitian kualitatif lebih fokus pada fenomena sosial dan berusaha untuk menggali perasaan serta persepsi para partisipan yang terlibat dalam studi tersebut. Pendekatan ini didasarkan pada keyakinan bahwa pengetahuan muncul dari konteks sosial dan pemahaman terhadap pengetahuan sosial merupakan proses ilmiah yang sah (legitimate). (Emzir 2011).

Penulisan ini menggunakan teknik pengumpulan data berupa *library Reasearch. Library Reasearch* merupakan Proses penelitian dilakukan dengan Mengumpulkan informasi dan data dari berbagai sumber yang ada di perpustakaan, seperti buku referensi, penelitian sebelumnya yang relevan, artikel, catatan, dan jurnal yang berkaitan dengan masalah yang sedang diteliti. Proses ini dilakukan secara terstruktur untuk mengumpulkan, menganalisis, dan menarik kesimpulan dari data dengan menggunakan metode atau teknik tertentu, dengan tujuan untuk menemukan solusi terhadap permasalahan yang ada (Sari 2020). Penelitian kualitatif ini akan menghasilkan analisis data yang berupa penjelasan mengenai situasi yang diteliti, yang disajikan dalam bentuk uraian naratif. (Rahmani Nur Ahmadi Bi 2022) Pendekatan kualitatif ini bertujuan untuk mendapatkan informasi lengkap tentang "Strategi Penguatan Database Nasabah Pada Perbankan Syariah.

D. HASIL DAN PEMBAHASAN

Salah satu kasus kejahatan siber pada perbankan syariah di Indonesia adalah peretasan sistem Bank Syariah Indonesia (BSI). Peretasan data nasabah telah menjadi masalah yang menonjol bagi Bank BSI, sehingga mendorong perhatian lebih dekat terhadap legalitas tindakan tersebut dan tindakan yang diperlukan untuk melindungi informasi nasabah dari ancaman dunia maya. Sebelum menjadi sasaran serangan peretasan pada 8 Mei 2023, sistem BSI sudah mengalami kegagalan fungsi. Dalam sistem perbankan, terdapat banyak sekali data sensitif seperti alamat, saldo rekening, riwayat transaksi, tanggal pembukaan rekening, rincian pekerjaan, dan sejumlah informasi lainnya yang akhirnya disusupi. Data klien yang bocor mencakup detail pribadi seperti nama, nomor telepon, alamat, modifikasi akun, aktivitas perdagangan,

tanggal dimulainya akun, catatan pekerjaan, dan sejumlah data lainnya. Tahapan atau rangkaian kronologi peretasan BSI:

a. Senin, 8 Mei 2023: Platform digital BSI, termasuk ATM dan Aplikasi BSI Mobile, saat ini tidak tersedia karena sedang dilakukan pemeliharaan oleh pihak bank.
b. Selasa, 9 Mei 2023: BSI mengeluarkan pernyataan bahwa pemulihan layanan ATM akan dilakukan secara bertahap dengan pemantauan terus menerus oleh Sekretaris Perusahaan Gunawan Arief Hartoyo. Sementara itu, aplikasi BSI Mobile tetap tidak dapat diakses karena terkadang dapat dibuka namun tidak dapat menyelesaikan transaksi. Perusahaan secara aktif berupaya mengatasi masalah ini dan memberikan pembaruan bila diperlukan.
c. Rabu, 10 Mei 2023: Penyebaran ransomware semakin mengkhawatirkan karena penyebab gangguan tersebut masih belum jelas dan belum ada pernyataan resmi yang dikeluarkan oleh BSI. Dilumpuhkannya layanan digital BSI berdampak besar pada provinsi Aceh yang sudah menerapkan sistem keuangan syariah. BSI merupakan pelaku pasar terbesar kedua setelah Bank Aceh, dan gangguan ini juga berdampak pada pembayaran biaya haji.
d. Kamis, 11 Mei 2023: Dalam jumpa pers sore harinya, Direktur Utama BSI Hery Gunardi mengumumkan layanan digital sudah kembali beroperasi normal meski bertahap. Gunardi menyebutkan adanya potensi tanda-tanda serangan siber yang berujung pada penutupan sementara sistem. Namun, dia menegaskan tuduhan tersebut harus dibuktikan kebenarannya. BSI bekerja sama dengan beberapa entitas, termasuk Bank Mandiri, Bank Indonesia, dan Otoritas Jasa Keuangan, untuk mempercepat proses pemulihan sistem.
e. Jumat, 12 Mei 2023: Hari terakhir jamaah haji melakukan pembayaran biaya haji, BSI melaporkan 95 persen jamaah sudah menyerahkan setoran. Untuk membantu mereka yang belum menyelesaikan pembayarannya, BSI mengumumkan rencana pembukaan 434 cabang selama akhir pekan. Selain itu, layanan dan fungsi digital BSI Mobile terus meningkat.
f. Sabtu, 13 Mei 2023: LockBit 3.0, kelompok peretas ransomware terkenal, telah mengumumkan bahwa mereka berhasil melancarkan serangan terhadap BSI dan berhasil memperoleh 1,5 TB data pribadi dari server organisasi.
g. Ahad-Senin, 14-15 Mei 2023: Layanan BSI saat ini sedang dalam proses pemulihan dan sebagian besar fungsinya berjalan seperti biasa. Batas waktu untuk LockBit 3.0 telah berlalu.
h. Selasa, 16 Mei 2023: Ada kecurigaan bahwa LockBit 3.0 telah mendistribusikan data yang dicurinya di web gelap. Informasi yang diambil terbanyak adalah pada 8 Mei 2023. Saham BRIS kembali mengalami kenaikan nilainya. BSI telah merilis pernyataan yang menyangkal adanya pelanggaran keamanan dan memastikan pelanggan bahwa data dan dana mereka aman.

i. Sabtu, 20 Mei 2023: Investigasi serangan siber terhadap Bank Syariah Indonesia (BSI) telah dimulai dan dilakukan secara menyeluruh oleh Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim Polri). Bareskrim Polri bekerja sama dengan berbagai pihak terkait, termasuk Badan Siber dan Sandi Negara (BSSN), untuk mengusut lebih dalam kejadian serangan siber tersebut. (Hukum et al. 2024)

Hacker mampu memanfaatkan bermacam-macam cara, contohnya pengelabuan, serangan *malicious software,* dan pembajakan data, supaya menjangkau data konsumen dan menghancurkan tatanan pada bank syariah. Pengelabuan/phising biasanya dilakukan dengan cara mengecoh menggunakan surat elektronik atau lokasi website tidak asli yang menipu konsumen agar memberikan keterangan data individu ataupun aset mereka. Hantaman *malicious software,* misalnya ransomware mampu menjangkiti tatanan serta mengunci data, memaksa konsumen atau bank untuk menebus agar dapat mengakses data kembali. Penjarah data pribadi merupakan salah satu bahayas signifikan. *Hacker* mengambil data nasabah buat bertindak terlarang. Zaman modern ini, sistem informasi konsumen bank syariah merupakan tanggung jawab bank syariah. Kejahatan rahasia data bisa merugikan kinerja maupun nama baik bank syariah. Beberapa ancaman kejahatan siber dapat dijelaskan sebagai berikut:

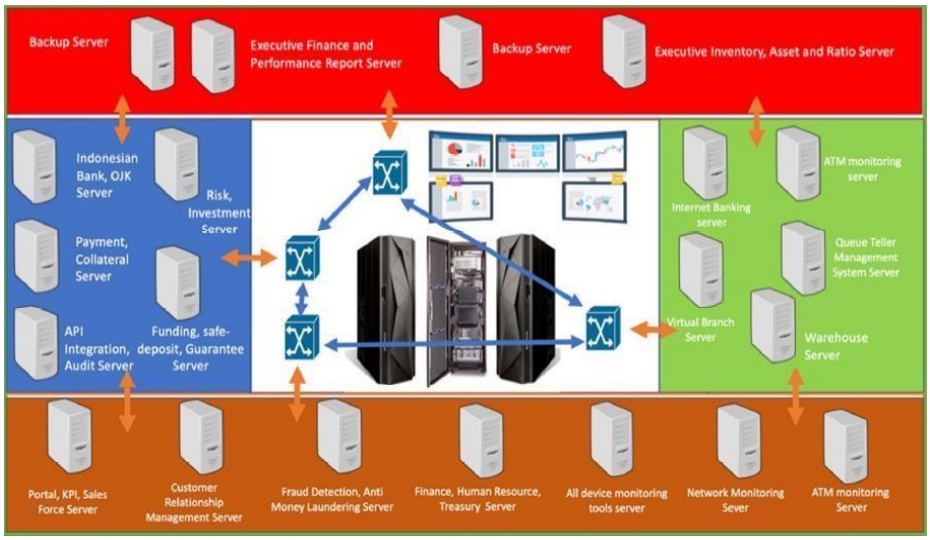
a. Serangan Malware dan Ransomware, Malicious Software merupakan instrumen lunak jahat yang disusun buat menghancurkan, menjangkiti, atau merampas informasi dari software komputer. Disisi lain, ransomware merupakan salah satu ragam malware yang mengunci data dimana korban diminta tebusan buat memulihkan portal ke data tersebut. Gempuran malware bisa dilakukan dengan beragam usaha, seperti melalui surat elektronik, link yang mencurigakan, maupun *download* dari lokasi website ilegal. Beberapa jenis malicious software yang sering ditemukan seperti trojan horse, worm, virus, serta spyware.
b. Pishing dan Social Engineering, Phishing adalah upaya untuk memperoleh informasi rahasia dari pengguna komputer dengan cara menipu mereka melalui pesan palsu yang tampak penting, yang bisa berupa email, situs web, atau bentuk komunikasi elektronik lainnya. Bila konsumen mengklik link dan memasang data pribadi misalnya panggilan konsumen dan *password, hacker* bakal mendapatkan pintu ke rekening konsumen tersebut. Gempuran phishing jua bisa dikerjakan memakai sapaan telepon ilegal atau amanat teks yang menipu konsumen buat menyerahkan data sendiri. Contohnya mencakup penipuan melalui *handphone,* dimana pelaku berlagak sebagai pegawai bank dan memohon data individu konsumen, atau gempuran yang melibatkan penyamaran personalitas, dimana *hacker* berusaha menganggap selaku pegawai bank buat memperoleh pintu ke algoritma komputer.
c. Kebocoran Data dan Pencurian Identitas: Kebocoran informasi juga dapat disebabkan oleh kesilapan personal, misal kelepasan gawai atau kelalaian dalam

mengatur informasi rentan. Perampasan data pribadi menyangkut pemakaian informasi seseorang, misal julukan, tanggal lahir, maupun ID Card, buat pengecohan serta jalan ilegal . (Faizal et al. 2023)

Kerugian lainnya yaitu seperti yang dikutip dari situs CNN Indonesia berdasarkan hasil wawancara pihak CNN Indonesia dengan Corporate Secretary BSI Gunawan Arif Hartoyo, bahwa sekitar 1200 unit ATM BSI dan kantor-kantor BSI mengalami gangguan (CNN Indonesia 2023). Selaku tanggapan atas kejadian yang menyusahkan corporate, bank syariah dapat menangkap prosedur taktik dalam memperkuat database nasabahnya atau konsumennya. Dalam upaya ini, perbankan syariah dapat merancang serangkaian kebijakan sebagai strategi untuk menguatkan pengamanan database , yaitu: Melakukan pencadangan (back up) data secara berkala dan terjadwal Pada basis data. Untuk mengurangi dampak serangan ransomware pada basis data, bank perlu melakukan pencadangan (backup) data secara rutin dan terjadwal. Langkah ini sangat penting agar, jika data utama dalam basis data rusak atau tidak dapat diakses akibat enkripsi oleh ransomware, data tersebut dapat dipulihkan.

Selain itu, sangat penting untuk tidak menyimpan salinan cadangan data hanya pada satu lokasi atau perangkat penyimpanan. Disarankan untuk mendistribusikan salinan cadangan dari basis data utama ke beberapa tempat penyimpanan yang berbeda, seperti cloud, server, perangkat keras (misalnya memori eksternal), dan lain-lain. Dengan demikian, data cadangan akan lebih terlindungi dan terhindar dari risiko kehilangan jika terjadi masalah pada salah satu tempat penyimpanan. (Of et al. 2023)

Dalam penelitian yang berjudul “Kesiapan Teknologi Informasi Perbankan Hadapi Revolusi Industri Era 4.0”, arsitektur teknologi perbankan yang dapat diterapkan oleh perbankan syariah sebagai upaya penguatan database nasabah dari serangan siber adalah sebagai berikut:



Gambar 2. Arsitektur Teknologi Perbankan

Pertama, pelaporan eksekutif, adalah arsitekture komputer yang mengamankan sistem operasi pelaporan. Didalamnya termuat summaries dari seluruh operasi yang ada didalam komputer bank. Cadangan server pula terdapat pada unit pelaporan eksekutif dan melaksanakan pencadangan atas *Primary Server.*
Kedua, sisi kanan dari desain teknologi yang berkaitan dengan nasabah. Arsitektur ini seperti berbagai server perlu dilakukan melalui pengamanan atau Cyber Security, karena secara sistem, server ini melayani langsung dengan eksternal jaringan atau internet. Penguatan dari arsitekture teknologi harus dapat memprakirakan gempuran eksternal jaringan.
Ketiga, sisi tengah dari desain komputer dirancang melalui penggunaan pengamanan perangkat keamanan. Perangkat keamanan seperti *Intrusion Detection System* berguna dalam mendeteksi serangan, *malware* dan lain-lain. Perangkat *Intrusion Prevention System* berguna dalam memproteksi serangan, seperti serangan jaringan, *malware* dan lain-lain. Selain itu juga dilengkapi dengan monitoring dari *Intrusion Detection* dan *Prevention*. Penguatan inilah yang harus dilakukan, karena perbankan harus melakukan perubahaan menghadapi revolusi industry era 4.0 maka hal ini perlu dilakukan.
Keempat, sisi kiri dari desain komputer adalah server Bank Indonesia dan OJK, server pembayaran dan jaminan, server risiko dan investasi, integrasi API dan server audit, pendanaan brankas, dan server penjaminan.
Kelima, sisi bawah dari desain komputer adalah portal, KPI, server tenaga penjualan, server manajemen hubungan pelanggan, deteksi penipuan, server anti pencucian uang, keuangan, sumber daya manusia, server perbendaharaan, server alat pemantauan semua perangkat, server pemantauan jaringan, server pemantauan ATM. (Syafie 2022)

Adanya pencadangan data atau backup data membantu perbankan syariah apabila terjadi krisis manajemen database akibat serangan siber. Jika terjadi serangan siber perbankan syariah masih dapat menyelamatkan data-data yang telah diretas dari pihak yang tidak bertanggungjawab, agar sistem operasiona perbankan syariah masih dapat berjalan. Meskipun demikian data yang dibobol tersebut harus tetap dipantau dan segera diperbaiki.

Penggunaan arsitektur tersebut diharapkan operasional perbankan syariah dapat berjalan dengan baik melalui sebuah sistem database yang terjaga secara sistematis, dan nasabah akan selalu yakin dan percaya dengan kemampuan perbankan syariah dalam menjaga kerahasiaan informasi dan aset-aset yang dimiliki nasabah untuk diamanahkan kepada perbankan syariah. Selain daripada itu, regulasi juga diperlukan dalam penguatan database nasabah perbankan syariah sebagai payung hukum atau kepastian hukum terhadap pihak-pihak yang bertanggungjawab dan sebagai pagar perlindungan agar tidak ada lagi pihak yang ingin melakukan peretasan data. Berikut

strategi lain dalam penguatan sistem database nasabah perbankan syariah melalui regulasi dari pemerintah:

Berdasarkan PasalPasal 40 ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, bank diwajibkan untuk Melindungi kerahasiaan informasi terkait nasabah dan simpanannya. Pasal ini secara jelas mengatur bahwa bank harus menjaga kerahasiaan data nasabah sebagai penyimpan dana. Sejalan dengan hal tersebut, Otoritas Jasa Keuangan (OJK) menerbitkan Surat Edaran No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data serta Informasi Pribadi Konsumen. Surat Edaran ini diterbitkan sehubungan dengan penerapan Peraturan OJK No. 1/POJK.07/2013 mengenai Perlindungan Konsumen di Sektor Jasa Keuangan. Surat Edaran OJK tersebut mewajibkan seluruh Pelaku Usaha Jasa Keuangan (PUJK), termasuk bank, untuk melindungi data pribadi konsumen dan melarang penyampaian data atau informasi pribadi tersebut kepada pihak ketiga dalam bentuk apa pun.

Data dan informasi konsumen yang harus dijaga kerahasiaannya, sesuai dengan Surat Edaran OJK, meliputi nama, alamat, tanggal lahir atau usia, nomor telepon, dan nama ibu kandung untuk individu, serta nama, alamat, nomor telepon, susunan direksi dan komisaris beserta identitas seperti KTP, paspor, atau izin tinggal, serta susunan pemegang saham untuk korporasi. Semua data ini harus dilindungi kerahasiaannya oleh lembaga perbankan dan tidak boleh diserahkan kepada pihak ketiga atau digunakan untuk tujuan selain yang telah disepakati, kecuali jika nasabah memberikan persetujuan tertulis atau sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, seperti yang diatur dalam Pasal 41 hingga 43 UU No. 10 Tahun 1998 tentang Perbankan (Abdul Rasyid 2017).

Secara spesifik, Hingga saat ini, belum ada undang-undang yang secara khusus mengatur tentang internet banking. Namun, jika dikaitkan dengan disiplin ilmu hukum, apabila suatu tindakan menyebabkan kerugian bagi orang lain, pihak yang melakukan tindakan tersebut wajib bertanggung jawab dan mengganti kerugian yang timbul akibat perbuatannya. Konsep ini dikenal dengan tanggung jawab kualitatif, yaitu tanggung jawab yang muncul karena seseorang memiliki kualitas tertentu. (Denisya, Budiartha, dan Putra 2024)

Dengan tiga strategi yang penulis tawarkan yaitu pencadangan data atau backup data nasabah, arsitektur teknologi perbankan, serta regulasi pemerintah. Maka, diharapkan perbankan syarah dapat mengimplementasikan konsep strategi penguatan database nasabah perbankan syariah yang telah ditawarkan oleh penulis supaya peristiwa yang terjadi dimasa lalu tidak terulang kembali dan proteksi sejak dini dari serangan siber.

E. KESIMPULAN

Strategi penguatan database pada perbankan syariah adalah hal yang harus diperhatikan sangat serius untuk menjaga integritas data nasabah serta memastikan keamanan dalam bertransaksi. Adapun strategi yang harus dilakukan bank adalah pencadangan data nasabah yang dilakukan secara rutin. Langkah ini diambil untuk memitigasi risiko kehilangan data akibat gagngguan teknis siber dan Rasomware. Arsitektur teknologi perbankan yang andal menjadi startegi untuk menguatkan database pada perbankan syariah, dimana pemanfaatan sistem berbasis cloud dan keamanan berlapis dapat menjamin ketersediaan dan kemanan data. Infrasturukutr yang kuat memungkinkan bank untuk mengelola data besar dengan efisien dan menghadapi risiko keamanan dengan cepat. Strategi terakhir adalah regulasi pemerintah yang ketat terkait keamananan data perlindungan nasabah. Dengan adanya database yang kuat maka amanah yang dipertanggungjawabkan oleh perbankan syariah dapat terlaksana. Keterbatasan dalam penelitian ini adalah memperoleh data serupa yang dialami PT. Bank Syariah Indonesia Tbk. Yaitu serangan siber terhadap system informasi (database) perbankan syariah Penulis menyarakan kepada pihak pemerintah untuk merumuskan undang- undang secara khusus yang mengatur mengenai internet banking guna menjaga keamanan database perbankan syraiah.

DAFTAR PUSTAKA

Abdul Rasyid. 2017. “Perlindungan Data Nasabah Perbankan.” *Business-Law.Binus.Ac.Id*. https://business-law.binus.ac.id/2017/07/31/perlindungan-datanasabah-perbankan/.

Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, dan Fried Sinlae. 2024. “Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT.” *Journal Zetroem* 6 (1): 114–19. https://doi.org/10.36526/ztr.v6i1.3376.

CNN Indonesia. 2023. “Kronologi Dugaan Serangan Siber Terhadap BSI, Transaksi Sempat Lumpuh.” *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/-20230511084123-192- 948087/kronologi-dugaan-serangan-siber-terhadap-bsi-transaksi-sempat- lumpuh

Denisya, Ni Putu, I Nyoman Putu Budiartha, dan I Made Aditya Mantara Putra. 2024. “Perlindungan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking.” *Jurnal Preferensi Hukum* 5 (2): 246–52. https://doi.org/10.22225/jph.5.2.8088.246-252.

Fahrurrozie, Rendra. 2023. *PERBANKAN SYARIAH DI INDONESIA - Sejarah Perbankan Syariah di Dunia dan di Indonesia : Perjalanan Menuju Sistem Keuangan yang Berkeadilan*. *Perbankan Syariah di Indonesia*. Bogor: Pustaka Amma Alamia, 36-52

Faizal, Muhazzab Alief, Zelyn Faizatul, Binti Nur Asiyah, dan Rokhmat Subagyo.

2023. "Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini." *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam* 5 (2): 87–100. https://doi.org/10.47435/asysyarikah.v5i2.2022.

Fatmala Putri, Dewi, dan Widya Ratna Sari. 2023. "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking." *Jurnal Ilmiah Ekonomi dan Manajemen* 1 (4): 173–81. https://doi.org/10.61722/jiem.v1i4.331.

Intan, Fajarlie Nadia. 2023. "15 juta data bank syariah indonesia diduga diretas, direktur utama: perlu pembuktian." *kompas tv*, 2023. https://www.kompas.tv/article/406513/15-juta-data-bank-syariah-indonesia-diduga-diretas-direktur-utama-perlu-pembuktian.

Muhammad Ghozali, Nora Liana, Cut Afra, dan Zulfadly Siregar, Nurfahni, Malahayati, Muhammad Hatta. 2024. "Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI)." *Cendekia: Jurnal Hukum, Sosial, dan Humaniora* 2 (4): 797–809. https://doi.org/10.5281/zenodo.13883603

Maulana, Bagus Restu, dan Nasrulloh Nasrulloh. 2024. "Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber." *EKSISBANK: Ekonomi Syariah dan Bisnis Perbankan* 8 (1): 76–91. https://doi.org/10.37726/ee.v8i1.1123

Maya Safitri, Eristya, Adelia Sefri Larasati, dan Syahroni Rizki Hari. 2020. "Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur." *Jurnal Ilmiah Teknologi Informasi dan Robotika* 2 (1): 12–16. https://doi.org/10.33005/jifti.v2i1.25.

Nurul Monika Larasati, dan Rayyan Firdaus. 2024. "Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan." *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika* 2 (4): 102–9. https://doi.org/10.61132/merkurius.v2i4.151.

Of, Simulation, Ransomware Attacks, Against The, Bank Syariah, dan Indonesia Database. 2023. "Terhadap Database Bank Syariah Indonesia Analysis and Simulation of Ransomware Attacks," no. September, 6–7.

Rahmani Nur Ahmadi Bi. 2022. *Metodologi Penelitian Kualitatif dan Kuantitatif*. Pertama. medan: PT Cahaya Rahmat RAHMANI, 6

Ramadhanti Achlina Tri Putri, dan Heru Sugiyono. 2024. "Tanggung Jawab Bank terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk)." *Jurnal Interpretasi Hukum* 5 (1): 682–90. https://doi.org/10.22225/juinhum.5.1.8318.682-690

Restika, Restika, dan Era Sonita. 2023. "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era

Digital." *Krigan: Journal of Management and Sharia Business* 1 (2): 25. https://doi.org/10.30983/krigan.v1i2.7929.

Sari, Milya. 2020. "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA." *NATURAL SCIENCE: Jurnal Penelitian Bidang IPA dan Pendidikan IPA,* 6 (1): 41–53.

Satrya Ilham Zharfan. 2024. "SERANGAN SIBER DALAM PERKEMBANGAN PERBANKAN DIGITAL DI INDONESIA." *Syntax Literate: Jurnal Ilmiah Indonesia* 09 (10): 5923–30. http://dx.doi.org/10.36418/syntax-literate.v9i10

Syafie, Syafie. 2022. "Kesiapan Teknologi Informasi Perbankan hadapi Revolusi Industri era 4.0." *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)* 9 (1): 533–46. https://doi.org/10.35957/jatisi.v9i1.1540.

Ujung, Adelia Marwah, Muhammad Irwan, dan Padli Nasution. 2023. "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi." *JISKA: Jurnal Sistem Informasi Dan Informatika* 1 (2): 44. http://jurnal.unidha.ac.id/index.php/jteksis.