Switch : Jurnal Sains dan Teknologi Informasi
Volume. 3, No. 1, Tahun 2025
e-ISSN : 3032-3320; dan p-ISSN : 3032-3339; Hal. 148-162
DOI: https://doi.org/10.62951/switch.v3i1.344
Available online at: https://journal.aptii.or.id/index.php/Switch

Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah

Abdullah Mubarak Lubis [1*], Gladis Jelita [2], Syafira Okta Vionna Wirya [3], Nurbaiti [4]
[1,2,3] Mahasiswa Fakultas Ekonomi dan Bisnis Islam, Universitas Negeri Sumatera Utara, Indonesia
[4] Dosen Fakultas Ekonomi dan Bisnis Islam, Universitas Negeri Sumatera Utara, Indonesia
Email: abdullubis1707@gmail.com [1] , gladisjamilah1107@gmail.com [2] , vionnawirya@gmail.com [3] , nurbaiti@uinsu.ac.id [4]

Alamat: Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara
Korespondensi penulis: abdullubis1707@gmail.com

Abstract. *Information technology (IT) has become a key element in the development of the financial industry, including Islamic banking. A primary challenge for IT management in Islamic banks is data security from cybercrime, which can damage the bank's reputation and customer trust. This study aims to further examine the challenges and efforts that Islamic banks can undertake to enhance IT security. The research methodology uses a qualitative approach with descriptive methods and literature review to describe the phenomenon in depth based on data and information from various relevant literature sources. The study's findings show that Islamic banks need to strengthen security through encryption, continuous monitoring, and employee training on cybersecurity. The conclusion of this study recommends that Islamic banks continue to raise awareness among employees and customers about security risks and ensure regulatory compliance. This research is expected to serve as a reference for Islamic banks in maintaining information security in the digital era.*

Keywords*: Challenges, Security, Information Technology, Islamic Bank Management*

Abstrak. Teknologi informasi (TI) telah menjadi elemen kunci dalam perkembangan industri keuangan, termasuk perbankan syariah Tantangan utama terhadap teknologi informasi manajemen bank syariah salah satunya ialah keamanan data dari kejahatan cyber yang dapat merusak reputasi bank syariah dan kepercayaan nasabah. Penelitian ini bertujuan untuk mengkaji lebih lanjut tantangan dan upaya yang dapat dilakukan oleh bank syariah dalam meningkatkan keamanan teknologi informasi. Metodologi penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif dan studi literatur untuk mendeskripsikan fenomena secara mendalam berdasarkan data dan informasi dari berbagai sumber literatur yang relevan. Hasil penelitian menunjukkan bahwa bank syariah perlu memperkuat keamanan dengan penerapan enkripsi, pemantauan berkelanjutan, serta pelatihan bagi karyawan tentang keamanan siber. Simpulan dari penelitian ini menyarankan bank syariah untuk terus meningkatkan kesadaran karyawan dan nasabah akan risiko keamanan serta memastikan kepatuhan terhadap regulasi. Penelitian ini diharapkan dapat menjadi referensi bagi bank syariah dalam menjaga keamanan informasi di era digital.

Kata kunci: Tantangan, Keamanan, Teknologi Informasi, Manajemen Bank Syariah

1. LATAR BELAKANG

Informasi didefinisikan sebagai data yang telah diproses, dan teknologi informasi adalah ilmu yang diperlukan untuk mengelolanya agar dapat diakses dengan akurat dan mudah. Menurut Darmawan (2012), data atau informasi ini dapat berupa teks, suara, foto, video, dan media lainnya. Teknologi informasi dan komunikasi (TIK), yang dikenal sebagai *Information and Communication Technology* (ICT) dalam bahasa Inggris, telah dengan cepat muncul sebagai komponen penting dalam kehidupan modern. (Sawitri, Astiti, and Fitriani 2019)

Received: Desember 17,2024; Revised: Desember 31, 2024; Accepted: Januari 04, 2024;
Published: Januari 07, 2025

Teknologi Salah satu faktor penting dalam pertumbuhan sektor keuangan, khususnya perbankan Islam, adalah teknologi informasi (TI). Pemanfaatan TI di bank-bank Islam tidak hanya menyederhanakan prosedur operasional, tetapi juga meningkatkan efektivitas manajerial dan aksesibilitas klien. Namun, seiring dengan kemajuan ini, masalah keamanan dan manajemen TI semakin kompleks. Bank-bank Islam harus menghadapi ancaman siber, pelanggaran data, dan kebutuhan untuk tetap mengikuti perkembangan teknologi yang cepat, sambil mempertahankan kepatuhan terhadap standar Syariah.

Bank-bank Islam harus lebih adaptif di dunia digital kontemporer untuk menawarkan layanan yang cepat, mudah, dan aman. Bekerja sama dengan perusahaan teknologi, khususnya di sektor telekomunikasi, adalah salah satu cara untuk mempromosikan digitalisasi perbankan. Sangat mungkin bahwa perusahaan-perusahaan telekomunikasi memiliki teknologi canggih yang dapat membantu dalam transisi digital perbankan. Dalam ranah perbankan online, masalah akses internet yang lambat adalah masalah yang umum. Karena itu, hanya 25% orang Indonesia yang memiliki akses ke layanan keuangan, meskipun sudah beroperasi selama beberapa dekade.

Setiap organisasi dan bisnis di negara ini terpengaruh oleh kemajuan industri dan bisnis yang dibawa oleh teknologi digital. Sebagai salah satu sektor keuangan yang bekerja sama dengan masyarakat, bank melihat transformasi digital ini sebagai peluang untuk secara konsisten menciptakan dan menemukan produk baru yang melengkapi kemajuan baik di bidang teknologi maupun ekonomi. Untuk menciptakan lingkungan yang sesuai dengan nilai-nilai Islam, terutama bagi komunitas Muslim, bisnis yang menggunakan bank dalam operasionalnya harus menganalisis dengan hati-hati sumber dan konsep yang digunakan. Untuk melindungi transaksi berbasis Syariah dan memberikan makna lebih besar pada nilai-nilai ibadah dalam kehidupan sehari-hari, sebuah organisasi diwajibkan.(Julianto and Helvira 2022)

Memastikan bahwa data dan informasi nasabah aman adalah salah satu tantangan terbesar dalam mengintegrasikan teknologi ke dalam layanan perbankan syariah. Bank syariah perlu memastikan bahwa sistem TI mereka dapat melindungi data nasabah dengan memadai, mengingat kompleksitas ancaman keamanan siber yang semakin meningkat. Kebutuhan nasabah yang mungkin tidak memiliki akses mudah ke teknologi juga harus diperhatikan oleh bank syariah, yang mengharuskan adanya upaya untuk menjaga layanan yang inklusif dan dapat diakses oleh semua sektor masyarakat.

Perlindungan data sensitif dari potensi serangan yang dapat merusak kerahasiaan dan integritasnya sangat bergantung pada keamanan siber. Data nasabah dan reputasi bank dapat menderita jika data nasabah terpapar akibat keamanan yang tidak memadai (Vebrianty 2021). Ketergantungan pada transaksi digital: Untuk meningkatkan produktivitas dan memberikan layanan yang lebih baik kepada nasabah, bank syariah semakin mengadopsi transaksi digital. Namun, transaksi digital juga menyediakan platform bagi serangan siber seperti malware, phishing, dan pencurian identitas. Untuk memastikan bahwa transaksi digital dalam perbankan syariah tetap aman dan dapat diandalkan, pemahaman tentang keamanan siber menjadi sangat penting (Sriwulan 2023). Integritas dan ketersediaan layanan: Manajemen likuiditas melibatkan lebih dari sekadar pemenuhan kebutuhan finansial; ini juga mencakup pemeliharaan ketersediaan dan integritas layanan. Serangan siber yang mengganggu proses manajemen likuiditas dan merusak atau menghentikan sistem operasional bank dapat mengakibatkan ketidakstabilan finansial dan penurunan kepercayaan nasabah. (Restika and Sonita 2023)

Keamanan teknologi informasi sangat penting bagi bank syariah, menurut penelitian sebelumnya. Mengingat bahwa sistem berbasis syariah umumnya memiliki aturan yang lebih ketat terkait transparansi dan kepatuhan, keamanan data dan informasi merupakan salah satu masalah utama yang dihadapi oleh bank syariah, menurut penelitian Harahap dan Rahman (2020). Namun, para ahli lainnya berpendapat bahwa pencurian identitas, keamanan siber, dan serangan terhadap data nasabah adalah beberapa masalah yang harus dihadapi oleh sistem informasi manajemen bank syariah karena berpotensi merusak kepercayaan konsumen.

Meskipun telah dilakukan berbagai langkah pencegahan, termasuk pemantauan yang lebih ketat dan enkripsi yang lebih baik, masih terdapat celah yang dapat menyebabkan serangan siber yang merugikan reputasi bank syariah dan merusak kepercayaan konsumen. Oleh karena itu, penelitian ini bertujuan untuk menyelidiki tantangan dan upaya yang dapat dilakukan oleh bank syariah untuk meningkatkan keamanan teknologi informasi, serta strategi yang dapat diterapkan untuk mengatasi berbagai masalah yang muncul di era digital saat ini.

2. KAJIAN TEORITIS

Tantangan

Kamus Besar Bahasa Indonesia mendefinisikan "tantangan" sebagai suatu keadaan atau benda yang dapat memotivasi seseorang untuk lebih tekun dalam menyelesaikan masalah, suatu rangsangan (untuk bekerja lebih giat, dan sebagainya). Memastikan bahwa data dan informasi nasabah aman adalah salah satu hambatan terbesar dalam mengintegrasikan teknologi ke dalam layanan manajemen perbankan syariah. Bank syariah harus memastikan bahwa solusi teknologi yang mereka terapkan dapat melindungi data nasabah dengan cukup baik mengingat kompleksitas ancaman keamanan siber yang semakin berkembang. Bank syariah juga harus mempertimbangkan kebutuhan nasabah mereka yang mungkin kesulitan dalam menggunakan teknologi, oleh karena itu mereka harus berupaya untuk menjaga layanan mereka tetap terbuka dan tersedia untuk semua lapisan masyarakat.(Ardista, Kusuma, and Munandar 2024)

Keamanan

Keamanan, menurut Faqih dan Emma (2016:6), adalah proses untuk melindungi aset informasi dari bahaya yang mungkin timbul. Oleh karena itu, keamanan membantu mengurangi berbagai potensi bahaya dan secara tidak langsung memastikan kelangsungan bisnis. Karena nasabah mempercayakan aset informasi mereka kepada bank, sangat penting untuk melindungi keamanan dan kerahasiaannya saat menggunakan internet banking. Keamanan merupakan komponen penting dari suatu sistem informasi. Secara umum, tim analis dan programmer telah melakukan pekerjaan yang baik dalam membangun sistem keamanan pada layanan perbankan online. Namun demikian, berbagai bentuk penipuan dan kegiatan kriminal masih terus terjadi meskipun sistem keamanan internet banking itu sendiri sudah ada. Oleh karena itu, untuk mengurangi kegiatan ilegal, sistem keamanan internet banking perlu diperbarui secara berkala.(Iqbal, Hasan, and Laili 2022)

Risiko yang terkait dengan keamanan siber di bank syariah meliputi ancaman terhadap operasional harian, risiko transaksi keuangan, dan serangan terhadap data nasabah. Kemampuan bank syariah untuk menangani masalah ini dengan mempertimbangkan aspek syariah akan berdampak signifikan terhadap kinerja manajemen likuiditas di institusi tersebut. Bank syariah harus menggunakan pendekatan terintegrasi yang mencakup teknologi, manajemen risiko, dan kepatuhan syariah untuk menjaga stabilitas keuangan dalam menghadapi ancaman keamanan siber. Sebuah kerangka kerja yang komprehensif

akan memastikan bahwa upaya manajemen likuiditas tidak hanya efektif tetapi juga mematuhi standar etika dan syariah.

Perlindungan data sensitif dari serangan yang dapat merusak kerahasiaan dan integritasnya sangat bergantung pada keamanan siber. Nasabah bisa menderita, begitu pula reputasi bank, jika data nasabah terekspos akibat keamanan yang tidak memadai. Ketergantungan pada transaksi digital: Untuk meningkatkan produktivitas dan memberikan layanan yang lebih baik kepada nasabah, bank syariah semakin mengadopsi transaksi digital. Namun, transaksi digital juga membuka peluang bagi serangan siber seperti malware, phishing, dan pencurian identitas. Oleh karena itu, pemahaman tentang keamanan siber menjadi sangat penting untuk menjamin keamanan dan keandalan transaksi digital di bank syariah.(Restika and Sonita 2023)

Teknologi Informasi

Teknologi Informasi adalah ilmu yang diperlukan untuk mengelola informasi agar informasi tersebut dapat dicari dengan mudah dan akurat, informasi dapat dikatakan sebagai data yang telah diolah. Data atau informasi tersebut dapat berupa tulisan, suara, gambar, video dan sebagainya. (Sawitri, Astiti, and Fitriani 2019)

Menciptakan sumber, memelihara saluran informasi, memilih dan mengirimkan informasi, secara selektif menerima informasi, menyimpan dan mengambil informasi, serta menggunakannya adalah semua komponen dari teknologi informasi. Industri perbankan mulai memanfaatkan teknologi berbasis komputer untuk mempermudah interaksi dengan nasabah seiring dengan berkembangnya teknologi informasi yang semakin canggih. Pada akhir 1970-an, istilah “teknologi informasi” mulai dikenal luas. Dulu, istilah ini lebih dikenal dengan penggunaan pengolahan data elektronik atau personal komputer. Kamus Oxford mendefinisikan teknologi informasi sebagai penyimpanan, pengolahan, dan penyebaran data, termasuk kata-kata, angka, dan gambar, serta perangkat elektronik, terutama personal komputer.(Niswah and Tambunan 2022)

Keunggulan kompetitif industri perbankan tercermin dalam berbagai atribut layanan, seperti fasilitas yang memudahkan nasabah, termasuk ATM, SMS banking, internet banking, mobile banking, dan layanan pribadi yang diberikan oleh karyawan bank. Karena teknologi digital adalah penyebab dari semua ini, setiap lembaga perbankan memiliki potensi untuk berkembang dan menjadi pemimpin, namun juga memiliki potensi untuk gagal dan tutup. Penggunaan layanan keuangan berbasis teknologi informasi dapat menimbulkan berbagai masalah, seperti kurangnya pengetahuan nasabah tentang teknologi

informasi dan kurangnya interaksi langsung antara nasabah dan karyawan, yang dapat merusak kepercayaan terhadap layanan berbasis teknologi. (Artiningrum 2022)

Prosedur bisnis industri perbankan telah terpengaruh secara cepat oleh teknologi informasi, terutama dengan berkembangnya internet. Salah satu area signifikan penerapan teknologi informasi adalah sektor perbankan itu sendiri. Sebagai hasilnya, bank-bank akan memanfaatkan teknologi informasi untuk meningkatkan layanan kepada nasabah dan masyarakat serta mendorong aktivitas operasional mereka. Teknologi informasi kini menjadi komponen penting dalam transaksi keuangan seiring dengan semakin meningkatnya penggunaan komputer dan perangkat mobile sebagai media transaksi. Hal ini juga didorong oleh meningkatnya penggunaan internet di Indonesia dan berkembangnya infrastruktur internetnya. (Nurzaqiah et al. 2024)

Manajemen Bank Syariah

Sebuah organisasi yang mengelola keuangan sesuai dengan prinsip-prinsip Islam dikenal sebagai bank syariah. Hal ini mencakup menghindari investasi dalam kegiatan haram, menerapkan sistem bagi hasil, dan mematuhi larangan riba (bunga). Sistem informasi manajemen di Bank Syariah Indonesia memudahkan penggunaan layanan seperti internet banking, yang aman dan mudah digunakan karena dilengkapi dengan beberapa lapisan keamanan dan layanan keamanan yang efektif untuk semua transaksi keuangan. Nasabah dapat memanfaatkan semua fitur dan layanan yang tersedia di internet banking dan mobile banking melalui sistem informasi manajemen. Karena setiap layanan terhubung dengan internet, nasabah dapat mengaksesnya dengan cepat. Tyoso (2016) menyatakan bahwa fungsi utama sistem informasi manajemen dalam sebuah organisasi adalah untuk memberikan umpan balik. Selain berfungsi sebagai alat pelaksanaan rencana, sistem informasi manajemen juga bertindak sebagai alat pengawasan dengan membandingkan hasil aktual dengan standar yang telah ditetapkan. (Julianto and Helvira 2022)

3. METODE PENELITIAN

Metodologi penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif dan studi literatur, yang secara khusus bertujuan untuk menghimpun dan menganalisis data dari berbagai publikasi ilmiah yang signifikan, mencakup jurnal-jurnal peer-reviewed, buku-buku akademik, serta berbagai sumber daring yang terpercaya. Proses penelitian ini dimulai dengan tahap pemilihan topik yang cermat dan relevan. Pendekatan ini bertujuan untuk mendeskripsikan fenomena secara mendalam berdasarkan data dan informasi dari berbagai sumber literatur yang relevan. Studi literatur dipilih sebagai metode

utama karena memberikan landasan teori yang kuat dan membantu menganalisis temuan-temuan yang telah ada mengenai keamanan teknologi informasi dalam perbankan syariah.

Menurut Danial dan Warsiak, studi literatur adalah prosedur di mana seorang peneliti mengumpulkan buku dan jurnal yang relevan dengan masalah atau tujuan penyelidikannya. Menurut Zed, proses penelitian studi literatur terdiri dari serangkaian kegiatan yang melibatkan pengumpulan, membaca, dan mendokumentasikan data perpustakaan serta pengelolaan sumber daya penelitian. (Zahra et al. 2024)Deskriptif secara karakteristik bermaksud membantu para peneliti untuk menggambarkan atau mempertajam penjelasan penelitian mereka agar nantinya dapat mempermudah dipahami oleh orang lain yang ingin mengetahui penelitian mereka.

Sumber data dalam penelitian ini terdiri dari artikel ilmiah, jurnal, buku, dan laporan penelitian terdahulu yang mengkaji keamanan teknologi informasi, tantangan, serta manajemen risiko di bank syariah. Literatur ini membantu mengidentifikasi permasalahan yang relevan terkait keamanan data serta ancaman siber yang dihadapi oleh bank syariah, termasuk pencurian identitas dan serangan terhadap data nasabah. Pengumpulan data dilakukan melalui metode studi dokumentasi, yang melibatkan penelusuran literatur terkait keamanan informasi pada bank syariah. Literatur yang relevan diseleksi berdasarkan kualitas, relevansi, dan kesesuaiannya dengan topik penelitian, sehingga data yang diperoleh dapat dianalisis dengan baik.

Data yang terkumpul dianalisis secara deskriptif dengan mengidentifikasi tema-tema utama terkait tantangan dan strategi keamanan yang dihadapi oleh bank syariah. Analisis ini meliputi tahap pengkodean, klasifikasi, dan penyimpulan data dari kajian literatur untuk menemukan pola dan kesamaan dalam strategi mitigasi risiko serta praktik keamanan yang diterapkan oleh bank syariah. Untuk menjaga validitas data, dilakukan triangulasi dengan membandingkan hasil kajian dari beberapa literatur untuk memastikan konsistensi informasi. Peneliti juga memeriksa kesesuaian konteks hasil kajian literatur dengan kondisi perbankan syariah di Indonesia saat ini.

4. HASIL DAN PEMBAHASAN

Industri perbankan, khususnya bank syariah, menghadapi tantangan baru dalam mengelola risiko teknologi informasi di era digital yang terus berkembang. Dari platform perbankan online hingga aplikasi perbankan seluler, teknologi informasi sangat penting bagi kelancaran operasional institusi perbankan syariah modern. Namun, selain keuntungan yang

ditawarkan oleh perkembangan teknologi ini, bank syariah juga menghadapi risiko dan tantangan yang serius.

Hukum Islam memberikan pedoman khusus bagi bank syariah, terutama dalam pengelolaan risiko. Mereka harus memastikan penggunaan teknologi informasi yang aman dan sesuai dengan hukum syariah untuk menjaga ketersediaan, kerahasiaan, dan integritas data nasabah. Dengan meningkatnya serangan siber dan munculnya taktik kejahatan yang semakin canggih, risiko terhadap keamanan dan privasi data nasabah semakin besar.

Dunia terus berkembang mengikuti perkembangan zaman. Baik negara maju maupun negara berkembang, seperti Indonesia, menunjukkan kemajuan dan perkembangan dalam bidang industri, infrastruktur, dan teknologi. (Irawan, Dianita, and Salsabila Mulya 2021)

Industri perbankan, terutama bank syariah, telah terpengaruh secara signifikan oleh perkembangan teknologi informasi. Manajemen risiko teknologi informasi menghadirkan tantangan khusus bagi bank syariah, yang didirikan berdasarkan prinsip-prinsip hukum Islam. Seiring dengan kemajuan teknologi, bank syariah menggunakan aplikasi perbankan seluler, platform perbankan internet, dan layanan digital lainnya untuk memenuhi kebutuhan nasabah dengan efektif. Namun, selain manfaat yang diberikan oleh teknologi modern, juga terdapat risiko dan tantangan serius dalam menjaga keamanan informasi dan mengelola risiko teknologi informasi secara efektif.

Bank syariah bertanggung jawab untuk menjaga kerahasiaan dan integritas informasi serta melindungi data nasabah. Namun, ancaman terhadap keamanan informasi semakin rumit dan berkembang seiring waktu. Serangan siber yang semakin terkoordinasi dan canggih oleh peretas yang terampil mengancam kerahasiaan data nasabah, integritas sistem, dan ketersediaan layanan. Bank syariah dihadapkan pada ancaman serius dari kejahatan siber seperti pencurian identitas, serangan malware, dan phishing.

Selain itu, tantangan lain yang dihadapi oleh bank syariah adalah pelanggaran privasi data dan peraturan yang ketat dalam pengelolaan informasi keuangan. Bank syariah harus mematuhi prinsip syariah dalam semua aspek operasional mereka, termasuk dalam pengelolaan risiko teknologi informasi. Penggunaan teknologi yang tidak sesuai dengan prinsip-prinsip syariah dapat memicu kekhawatiran mengenai privasi dan keamanan informasi nasabah.

Tantangan Teknologi Informasi Pada Manajemen Bank Syariah

Serangan siber oleh peretas yang berpengalaman merupakan salah satu ancaman terbaru. Peretas dapat mengakses data nasabah dan merusak sistem keuangan dengan berbagai teknik, termasuk phishing, serangan malware, dan pencurian identitas. Serangan

phishing menggunakan email atau situs web palsu untuk menipu pengguna agar mengungkapkan informasi pribadi atau keuangan. Serangan malware seperti ransomware dapat menginfeksi sistem dan mengenkripsi data, memaksa bank atau nasabah untuk membayar tebusan guna mendapatkan kembali akses. Ancaman besar lainnya adalah pencurian identitas, di mana peretas mencuri identitas nasabah dan menggunakannya untuk tujuan penipuan atau kegiatan ilegal.

Pelanggaran privasi data adalah ancaman lain yang harus dihadapi oleh bank syariah. Data nasabah telah menjadi aset penting di era digital yang perlu dilindungi. Pelanggaran privasi data dapat menimbulkan kerugian finansial yang besar dan merusak reputasi bank syariah. Ancaman ini dapat berasal dari serangan siber atau kejadian internal seperti kebocoran data atau akses yang tidak sah oleh karyawan yang ceroboh. Pengelolaan privasi data yang efektif sangat penting untuk mempertahankan kepercayaan dan loyalitas nasabah.

Untuk memastikan bahwa semua transaksi dan operasi mematuhi aturan Syariah, masalah ini memerlukan pengawasan dan pengendalian yang ketat terhadap aplikasi perbankan seluler dan sistem perbankan online. Bank syariah harus menerapkan rencana keamanan yang menyeluruh untuk mengatasi risiko dan tantangan ini. Hal ini meliputi penerapan langkah-langkah keamanan yang kuat seperti enkripsi data, pemantauan jaringan yang berkelanjutan, pelatihan keamanan bagi staf, dan audit keamanan secara berkala. Membangun kerangka kerja yang efektif untuk mengatasi ancaman teknologi informasi juga memerlukan kerja sama dengan lembaga keamanan dan regulator. Berikut adalah beberapa rincian mengenai kesulitan yang dihadapi oleh bank syariah: (Faizal et al. 2023)

a. Kejahatan Cyber

Kejahatan siber dapat memiliki dampak yang merusak dan serius pada teknologi informasi bank syariah, baik bagi bank maupun nasabahnya. Pencurian data, serangan peretasan, penipuan online, dan penyebaran malware adalah contoh kejahatan siber, yang melibatkan penggunaan teknologi dan jaringan komputer untuk melakukan tindakan ilegal atau merugikan. Pemahaman yang mendalam tentang berbagai jenis kejahatan siber ini sangat penting dalam upaya menjaga integritas data keuangan dan melindungi sistem perbankan syariah.

Soesanto et al. mengungkapkan bahwa peningkatan kejahatan siber telah mencapai tingkat yang mengkhawatirkan. Legislasi positif konvensional tidak cukup untuk memerangi aktivitas ilegal di dunia maya. Hal ini disebabkan oleh berbagai hubungan antara lima elemen terkait: hukum, reaksi publik terhadap kejahatan, serta pelaku dan korban kejahatan tersebut. Meskipun hukum sangat penting dalam

pencegahan dan penanganan kejahatan, menyusun peraturan yang dapat beradaptasi dengan perubahan cepat di berbagai sektor, termasuk teknologi informasi, merupakan tugas yang sulit. Untuk mengatasi tantangan kejahatan siber, diperlukan kolaborasi antara berbagai sektor, termasuk sektor publik, swasta, penegak hukum, dan pemerintah. Selain itu, memperkuat kerangka hukum yang sesuai dan memanfaatkan teknologi keamanan siber yang canggih sangat penting dalam menghadapi ancaman yang terus berkembang. (Ray et al. 2024)

Pencegahan lebih baik daripada pemulihan dalam menghadapi kejahatan siber. Oleh karena itu, bank syariah harus secara proaktif mengidentifikasi dan mengurangi risiko kejahatan siber dengan menggunakan teknologi keamanan canggih, kebijakan dan prosedur yang ketat, pelatihan yang berkelanjutan, serta peningkatan kesadaran akan keamanan.

b. Phising dan Social Engineering

Social engineering sering menggunakan teknik rekayasa sosial dan phishing untuk melakukan kejahatan terhadap nasabah bank syariah. Phishing adalah praktik mengirimkan pesan penting palsu yang bisa berupa email, halaman web, atau komunikasi elektronik lainnya untuk menipu pengguna komputer agar mengungkapkan informasi pribadi. (Keuangan, Islam, and Syariah 2022)

Salah satu teknik yang populer untuk penipuan online adalah phishing. Sebagai contoh, untuk mencuri informasi sensitif dari nasabah, seorang penjahat dunia maya dapat mengirimkan pesan palsu yang meniru organisasi tepercaya, seperti bank syariah, ke alamat email atau platform media sosial lainnya. Pesan tersebut sering menyertakan tautan ke situs web palsu yang telah dibuat oleh penjahat dunia maya untuk meniru situs yang asli. Jika nasabah mempercayai pesan tersebut dan mengikuti instruksi dengan mengklik tautan dan memasukkan informasi pribadi seperti nama, kata sandi, atau email, penjahat dunia maya dapat mengakses akun nasabah dan mencuri data mereka. Namun, penipuan jenis ini juga bisa dilakukan melalui panggilan telepon atau pesan teks yang menipu nasabah untuk memberikan informasi pribadi. Edukasi pengguna, perlindungan phishing di level email, perangkat lunak anti-phishing, dan penggunaan sistem OTP (One-Time Password) dalam layanan keuangan adalah beberapa cara yang efektif untuk mencegah serangan semacam ini. (Muftiadi, Agustina, and Evi 2022)

Penjahat siber menggunakan social engineering, sebuah metode manipulasi psikologis, untuk mengendalikan orang dan mendapatkan data atau sistem yang sensitif. Untuk memperoleh informasi yang mereka butuhkan, penyerang menggunakan teknik

manipulasi seperti memanfaatkan kepercayaan, membangkitkan perasaan, atau memanfaatkan kurangnya kesadaran tentang keamanan. Serangan social engineering meliputi serangan pencurian identitas, di mana penyerang berusaha menyamar sebagai karyawan bank untuk mendapatkan akses ke sistem internal, dan penipuan telepon, di mana penyerang berpura-pura menjadi petugas bank dan meminta informasi pribadi dari nasabah. Untuk membantu nasabah melindungi diri dari penipuan tersebut, upaya dapat dilakukan untuk mengedukasi mereka mengenai cara mengenali tanda-tanda peringatan dari penipuan yang dilakukan oleh penyerang.

c. Serangan Malware dan Ransomware

Keamanan jaringan berfungsi sebagai penghalang untuk mencegah serangan virus pada data pengguna. Setiap jaringan memerlukan sistem pendeteksi untuk meningkatkan keamanan dan melindungi data dari pencurian. Sistem pendeteksi keamanan jaringan otomatis untuk menemukan semua risiko dan mampu mengidentifikasi berbagai jenis serangan. Sistem deteksi intrusi, atau IDS, adalah alat yang digunakan untuk mendeteksi ketidakteraturan dalam jaringan bisnis.

Serangan yang menggunakan malware dan ransomware pada sistem TI bank syariah dapat berdampak serius pada keamanan data dan kelangsungan operasional bank. Informasi pribadi nasabah yang sangat sensitif, khususnya data keuangan yang dapat digunakan untuk penipuan atau dijual di pasar gelap, dapat dicuri akibat serangan ini. Malware adalah perangkat lunak yang dirancang untuk merusak, menginfeksi, atau mencuri informasi dari sistem komputer. Sementara itu, ransomware adalah jenis perangkat lunak yang mengenkripsi data di komputer korban dan kemudian meminta pembayaran untuk membuka kunci data tersebut. Melindungi sistem perbankan syariah dan informasi pribadi nasabah memerlukan pemahaman yang mendalam tentang serangan-serangan ini. (Madakam, Ramaswamy, and Tripathi 2015)

Serangan malware dapat terjadi melalui berbagai cara, termasuk mengirimkan tautan mencurigakan melalui email atau mengunjungi situs web berisiko. Serangan malware dapat mengendalikan sistem dari jarak jauh, merusak file, dan mencuri data. Jika serangan malware terjadi pada bank syariah, bank tersebut dapat mengalami kerugian finansial yang besar, kehilangan data nasabah, dan kerusakan reputasi.

Ransomware adalah jenis perangkat lunak berbahaya yang, kecuali korban membayar tebusan, mengancam untuk menghapus atau memblokir data atau sistem penting. Meskipun awalnya ditujukan kepada individu, serangan ransomware oleh peretas telah meningkat dalam frekuensi dan kompleksitas dalam beberapa tahun

terakhir. Organisasi kriminal melakukan serangan ini dengan membobol jaringan perusahaan menggunakan intelijen yang telah mereka peroleh. Beberapa serangan bahkan begitu canggih sehingga para pelaku dapat menghitung jumlah tebusan yang diminta menggunakan data keuangan internal. (Nurul Monika Larasati and Rayyan Firdaus 2024)

d. Kurangnya kesadaran dan keamanan

Salah satu masalah yang harus dihadapi oleh bank syariah adalah kurangnya kesadaran dan keamanan. Meskipun bank syariah telah menerapkan langkah-langkah keamanan, masih ada kemungkinan bahwa beberapa karyawan atau nasabah tidak menyadari atau tidak sepenuhnya memahami prosedur keamanan berisiko tinggi, yang membuka peluang untuk serangan siber. Nasabah menjadi sasaran yang mudah bagi penyerang ketika mereka ceroboh dengan informasi pribadi mereka atau gagal mengenali tanda-tanda peringatan dari penipuan phishing. Di sisi lain, ketidaktahuan karyawan dapat mengakibatkan kesalahan manusia yang mempermudah eksploitasi kerentanannya oleh peretas. Pemberian pelatihan keamanan kepada nasabah dan karyawan bank syariah sangat penting untuk mengatasi masalah ini, karena dapat meningkatkan kesadaran tentang risiko keamanan dan mengajarkan mereka cara melindungi diri ketika ancaman tersebut terjadi.

Keamanan Teknologi Informasi Pada Bank Syariah

Salah satu komponen terpenting yang dapat melindungi sistem perbankan dan data nasabah adalah sistem keamanan yang tepat. Penilaian dan identifikasi risiko merupakan langkah pertama dalam menerapkan sistem keamanan yang sesuai. Bank syariah harus melakukan analisis risiko secara menyeluruh untuk menemukan potensi risiko dan kelemahan dalam sistem yang mereka gunakan guna mengurangi berbagai jenis serangan. Oleh karena itu, bank syariah harus memiliki pemahaman yang mendalam mengenai potensi risiko dan tantangan serta ruang lingkup perbankan, teknologi informasi, dan infrastruktur.

Langkah kedua adalah bagi bank syariah untuk memiliki pengawasan dan pemantauan yang aktif agar tidak melewatkan serangan atau aktivitas mencurigakan dalam sistem mereka. Dengan adanya pemantauan dan pengawasan yang aktif, bank syariah dapat merespons dengan cepat ketika serangan terjadi dan mengurangi dampak yang mungkin timbul.

Fase ketiga adalah bagi bank syariah untuk menjalankan kampanye kesadaran dan pelatihan keamanan yang berkelanjutan yang melibatkan semua pihak terkait dalam pemeliharaan sistem keamanan. Karyawan harus menerima pelatihan keamanan secara

reguler yang mencakup topik seperti praktik keamanan terbaik, serangan terbaru, dan langkah-langkah yang harus diambil jika terjadi masalah keamanan. Nasabah juga perlu diberi informasi tentang prosedur keamanan dalam menggunakan perangkat perbankan online, tanda-tanda serangan, dan bahaya keamanan yang mungkin mereka hadapi.

Menjaga kepatuhan terhadap peraturan yang relevan dan kebijakan privasi bergantung pada fase terakhir. Bank syariah diharuskan untuk memahami dan mematuhi peraturan privasi serta standar kepatuhan yang ditetapkan oleh badan pengatur, termasuk perlindungan data pribadi dan keamanan informasi. Implementasi kontrol keamanan yang tepat dan prosedur kepatuhan sangat penting untuk memenuhi harapan nasabah terkait privasi dan keamanan serta menjaga reputasi bank syariah. Salah satu langkah terpenting dalam melindungi bank syariah dari ancaman teknologi informasi saat ini adalah dengan menerapkan sistem keamanan yang sesuai. Dengan demikian, bank syariah dapat mengurangi kemungkinan serangan dan meningkatkan keamanan sistem mereka.(Faizal et al. 2023)

5. KESIMPULAN DAN SARAN

Perkembangan teknologi informasi telah membawa dampak yang signifikan pada sektor perbankan, termasuk bank-bank syariah. Bank syariah, yang didasarkan pada prinsip-prinsip syariat Islam, menghadapi tantangan khusus dalam mengelola risiko teknologi informasi. kejahatan siber dapat memiliki dampak yang serius dan merugikan, baik bagi bank itu sendiri maupun nasabahnya. Kejahatan siber melibatkan penggunaan teknologi dan jaringan komputer untuk melakukan kegiatan ilegal atau merugikan. Oleh karena itu, bank syariah harus secara proaktif mengidentifikasi dan mengurangi risiko kejahatan siber melalui penggunaan teknologi keamanan yang canggih. Phising merupakan metode umum yang digunakan untuk penipuan online. upaya untuk mencegahnya dengan melakukan edukasi pengguna. Social engineering adalah metode manipulasi psikologis yang digunakan oleh penjahat siber untuk memanipulasi manusia dan mendapatkan akses ke sistem atau informasi yang sensitif. Upaya yang dapat dilakukan dengan mengedukasi nasabah memberitahu tanda-tanda penipuan yang dilakukan oleh penyerang agar dapat melindungi dirinya dari penipuan tersebut. Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, menginfeksi, atau mencuri data dari sistem komputer. Sementara itu, ransomware adalah jenis malware yang mengenkripsi data pada sistem korban dan meminta tebusan untuk mengembalikan akses ke data tersebut. Kurangnya kesadaran dan keamanan menjadi salah satu tantangan bagi bank syariah yang harus diatasi. Upaya yang dapat

dilakukan dengan memberikan pelatihan edukasi terkait keamanan dan kesadaran kepada pihak yang bersangkut paut.

Langkah yang dapat dilakukan untuk menjaga keamanan teknologi informasi pada bank syariah ialah dengan menerapkan sistem keamanan yang tepat yaitu, identifikasi dan evaluasi risiko, bank syariah harus memiliki pengawasan dan pemantauan yang aktif dan tidak lalai, bank syariah mengadakan pelatihan dan kesadaran keamanan yang terus-menerus dalam melibatkan semua pihak terkait dalam menjaga sistem keamanan, dan menjaga kepatuhan terhadap regulasi dan kebijakan privasi yang berlaku.

Penulis ingin mengucapkan terimakasih kepada pembaca artikel ini yang membahas tentang tantangan dan keamanan teknologi informasi pada manajemen bank syariah. Semoga dapat menambah wawasan baru kepada pembaca. Penulis menyadari dalam hal penelitian dan penulisan jurnal ini masih jauh dari kata sempurna dan banyak kekurangan. Penelitian ini memiliki keterbatasan karena menggunakan metode studi literatur sehingga tidak dapat menggambarkan kondisi keamanan teknologi informasi di bank syariah secara langsung. Untuk penelitian selanjutnya, disarankan agar melakukan studi lapangan atau survei langsung untuk mendapatkan data empiris terkait implementasi keamanan teknologi informasi di bank syariah serta respons nasabah terhadap langkah-langkah keamanan yang telah diterapkan. Penelitian selanjutnya juga dapat mengeksplorasi lebih dalam tentang strategi adaptasi terhadap serangan siber yang muncul seiring perkembangan teknologi digital. Penulis berharap untuk penulis selanjutnya dapat memberikan pembahasan yang lebih lengkap dan lebih mudah dipahami oleh pembaca.

DAFTAR REFERENSI

Ardista, R., Kusuma, A. P., & Munandar, A. N. I. (2024). Manajemen sumber daya manusia di bank syariah: Tantangan dan peluang dalam era digital. *Jurnal Ekonomika dan Bisnis (JEBS), 4*(4), 634–639. https://doi.org/10.47233/jebs.v4i4.1932

Artiningrum, N. Z. (2022). Analisis kesiapan Bank Syariah Indonesia dalam menghadapi perkembangan layanan jasa keuangan berbasis teknologi informasi. *Journal of Financial Economics & Investment, 2*(3), 153–165. https://doi.org/10.22219/jofei.v2i3.19916

Faizal, M. A., Zelyn, F., Nur Asiyah, B., & Subagyo, R. (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/asy-syarikah.v5i2.2022

Iqbal, M., Hasan, A., & Laili, I. (2022). Pengaruh teknologi informasi, manfaat, keamanan, dan fitur layanan terhadap minat nasabah menggunakan internet banking (Studi kasus

pada nasabah Bank BNI Syariah Kota Tangerang Selatan). *Jurnal Masharif Al-Syariah: Jurnal Ekonomi dan Perbankan Syariah, 7*(1), 333–356. Retrieved from http://journal.um-surabaya.ac.id/index.php/Mas/index

Irawan, H., Dianita, I., & Mulya, A. D. S. (2021). Peran Bank Syariah Indonesia dalam pembangunan ekonomi nasional. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam, 3*(2), 147–158. https://doi.org/10.47435/asy-syarikah.v3i2.686

Julianto, J., & Helvira, R. (2022). Peran sistem informasi manajemen Bank Syariah Indonesia dalam membantu peningkatan perekonomian dan bisnis di era digital. *OIKONOMIKA: Jurnal Kajian Ekonomi dan Keuangan Syariah, 3*(2), 144–155. https://doi.org/10.53491/oikonomika.v3i2.637

Keuangan, J. L., Bisnis Islam, & Perbankan Syariah. (2022). Asy-Syarikah Asy-Syarikah. *Jurnal Asy-Syarikah, 4*(1), 81–92.

Larasati, N. M., & Firdaus, R. (2024). Analisis bahaya serangan ransomware terhadap layanan perbankan. *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, 2*(4), 102–109. https://doi.org/10.61132/merkurius.v2i4.151

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, 3*(5), 164–173. https://doi.org/10.4236/jcc.2015.35021

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: Analisis ancaman phishing terhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik, 1*(2), 60–65. https://doi.org/10.55904/hexatech.v1i2.346

Niswah, K., & Tambunan, K. (2022). Analisis strategi manajemen Bank Syariah Indonesia dalam meningkatkan market share melalui pemanfaatan teknologi informasi. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam, 3*(6), 1272–1289. https://doi.org/10.47467/elmal.v3i6.1210

Nurzaqiah, N., Ainulyaqin, M. H., Achmad, L. I., & Edy, S. (2024). Analisis manajemen risiko keamanan self-service technology perbankan syariah. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam, 5*(7), 3564–3578. https://doi.org/10.47467/elmal.v5i7.3379

Ray, S., Das, J., Pande, R., & Nithya, A. (2024). [Title not provided]. *Journal Title, 6*(1), 195–222. https://doi.org/10.1201/9781032622408-13

Restika, R., & Sonita, E. (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

Sawitri, E., Astiti, M. S., & Fitriani, Y. (2019). Hambatan dan tantangan pembelajaran berbasis teknologi informasi dan komunikasi. *Prosiding Seminar Nasional Pendidikan Program Pascasarjana Universitas PGRI Palembang*, 202–213.

Zahra, A., Afiyatni, N., Lie, A. Y., Rachman, I. F., & Universitas Siliwangi. (2024). Strategi literasi dalam menanamkan pendidikan karakter untuk mengatasi tantangan teknologi informasi dan komunikasi pada era disrupsi. *Jurnal Penelitian Pendidikan Indonesia, 1*(3), 435–442.