Restika , Era sonita
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929

Krigan:
Journal of Management and Sharia Business
e-ISSN: 3025-7603 p-ISSN:

ORIGINAL ARTICLE OPEN ACCES

TANTANGAN KEAMANAN SIBER DALAM MANAJEMEN LIKUIDITAS BANK SYARIAH : MENJAGA STABILITAS KEUANGAN DI ERA DIGITAL

Restika[1], Era Sonita [2]

***Korespondensi :**
Email :
restik426@gmail.com
3ras0nitha@gmail.com

Afiliasi Penulis :
[1, 2] Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, *Indonesia*

Riwayat Artikel :
Penyerahan : 17 Oktober 2023
Revisi : 23 November 2023
Diterima : 4 Desember 2023
Diterbitkan : 30 Desember 2023

Kata Kunci :
Keamanan Siber, Manajemen Likuiditas Bank Syariah, Stabilitas Keuangan, Era Digital

Keyword :
Keamanan Siber, Manajemen Likuiditas Bank Syariah, Stabilitas Keuangan, Era Digital

Abstrak

Penelitian ini mengeksplorasi tantangan keamanan siber yang dihadapi oleh lembaga keuangan, khususnya bank syariah, dalam konteks manajemen likuiditas guna menjaga stabilitas keuangan di era digital. Era digital menandai transformasi lanskap keuangan yang memberikan kemudahan tetapi juga menimbulkan risiko keamanan siber yang signifikan. Bank syariah, sebagai entitas keuangan yang mengimplementasikan prinsip-prinsip syariah, terutama rentan terhadap serangan siber yang dapat mengancam likuiditas dan stabilitas keuangan mereka. Penelitian ini mencakup latar belakang mendalam tentang serangan siber dan manajemen likuiditas di bank syariah. Dengan mempertimbangkan teori-teori terkini dan studi kasus terkait, penelitian ini menganalisis dampak serangan siber terhadap likuiditas dan stabilitas keuangan bank syariah. Sebagai bagian dari metodologi penelitian, studi literatur mendalam digunakan untuk mengidentifikasi tren, tantangan, dan strategi terkait keamanan siber dalam manajemen likuiditas. Temuan penelitian ini memberikan wawasan mendalam tentang bagaimana bank syariah dapat menghadapi dan merespons tantangan keamanan siber, serta strategi yang dapat diterapkan untuk mempertahankan stabilitas keuangan di era digital. Implikasi praktis dan rekomendasi untuk lembaga keuangan serupa turut dibahas, memberikan kontribusi pada pemahaman praktis dan kebijakan terkait manajemen likuiditas dan keamanan siber.Penelitian ini memberikan pemahaman yang lebih mendalam tentang hubungan antara keamanan siber dan stabilitas keuangan, memberikan kerangka kerja yang diperlukan bagi bank syariah dan lembaga keuangan lainnya untuk menghadapi tantangan kompleks ini.

.

Abstract

This research explores the cyber security challenges faced by financial institutions, especially Islamic banks, in the context of liquidity management to maintain financial stability in the digital era. The digital era marks a transformation of the financial landscape that provides convenience but also poses significant cybersecurity risks. Islamic banks, as financial entities that implement sharia principles, are especially vulnerable to cyber attacks that can threaten their liquidity and financial stability. This research includes an in-depth background on cyber attacks and liquidity management in Islamic banks. By considering current theories and related case studies, this research analyzes the impact of cyber attacks on the liquidity and financial stability of Islamic banks. As part of the research methodology, an in-depth literature study was used to identify cybersecurity-related trends, challenges and strategies in liquidity management. The findings of this research provide in-depth insight into how Islamic banks can face and respond to cyber security challenges, as well as strategies that can be implemented to maintain financial stability in the digital era. Practical implications and recommendations for similar financial institutions are discussed, contributing to practical and policy understanding regarding liquidity management and cyber security. This research provides a deeper understanding of the relationship between cyber security and financial

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

stability, providing the necessary framework for Islamic banks and other financial institutions to face this complex challenge.

.

Pendahuluan

Dalam era digital yang semakin maju, perbankan syariah menghadapi tantangan yang semakin kompleks terutama dalam pengelolaan likuiditas. Manajemen likuiditas yang efektif menjadi kunci untuk menjaga stabilitas keuangan bank syariah, namun kemajuan teknologi juga membawa risiko baru yang signifikan, terutama dalam bentuk keamanan siber. Keamanan siber menjadi fokus utama karena bank syariah menggunakan platform digital untuk melakukan transaksi, menyimpan data pelanggan, dan menjalankan operasional sehari-hari.

Pertumbuhan teknologi informasi dan komunikasi telah memberikan peluang besar bagi perkembangan perbankan syariah. Namun, seiring dengan manfaatnya, keamanan siber menjadi ancaman yang serius yang dapat mengganggu operasional dan stabilitas keuangan bank syariah. Peningkatan aksesibilitas melalui platform digital memberikan peluang bagi peningkatan layanan, tetapi juga meningkatkan risiko terhadap serangan siber yang dapat merusak integritas data dan kepercayaan nasabah. (Munawarah, H., Yusuf, M., & Komarudin 2022); (Raharjo 2021) Manajemen likuiditas di bank syariah memiliki kompleksitas tersendiri karena adanya prinsip-prinsip syariah yang mengatur operasionalnya. Oleh karena itu, tantangan keamanan siber tidak hanya berkaitan dengan aspek teknologi, tetapi juga dengan perlindungan terhadap prinsip-prinsip syariah dalam menjaga keamanan dan kepercayaan nasabah. (Abdul, A. R., Mandiri, D. P., Astuti, W., & Arkoyah 2022).

Keamanan siber di bank syariah melibatkan risiko yang beragam, termasuk serangan terhadap data nasabah, ancaman terhadap operasional harian, dan risiko terhadap transaksi keuangan. Keberhasilan manajemen likuiditas di bank syariah akan sangat dipengaruhi oleh sejauh mana bank dapat mengelola dan mengatasi tantangan ini dengan mempertimbangkan aspek syariah. Untuk menjaga stabilitas keuangan dalam menghadapi tantangan keamanan siber, bank syariah perlu mengadopsi pendekatan terintegrasi yang mencakup aspek teknologi, manajemen risiko, dan kepatuhan syariah. Sebuah kerangka kerja yang holistik akan memastikan bahwa upaya untuk mengelola likuiditas tidak hanya efisien tetapi juga mematuhi prinsip-prinsip etika dan syariah. (Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki 2022).

Pentingnya keterkaitan antara manajemen likuiditas dan keamanan siber adalah aspek yang perlu dicermati secara lebih mendalam. Kondisi likuiditas yang baik memerlukan perlindungan terhadap serangan siber yang dapat mempengaruhi operasional dan kepercayaan pelanggan.

Dengan melihat tren global dalam keamanan siber di sektor keuangan, penting bagi bank syariah untuk memahami dan mengadopsi praktik terbaik yang relevan dengan konteks perbankan syariah. Analisis terhadap tren global ini dapat memberikan wawasan yang berharga untuk mengatasi tantangan keamanan siber secara efektif.

Tantangan keamanan siber dalam manajemen likuiditas memiliki implikasi yang signifikan terhadap praktik perbankan syariah. Keberhasilan manajemen likuiditas tidak hanya tergantung pada ketepatan strategi keuangan, tetapi juga pada bagaimana bank menghadapi dan mengatasi ancaman keamanan siber.Penelitian ini akan merinci literatur terkait keamanan siber, khususnya dalam konteks perbankan syariah. Kajian literatur ini akan melibatkan pemahaman mendalam tentang tantangan keamanan siber yang unik dalam operasional bank syariah dan bagaimana literatur saat ini mengusulkan strategi untuk mengatasi tantangan tersebut.

Dalam konteks dinamika perbankan syariah yang semakin terdigitalisasi, terdapat berbagai tantangan keamanan siber yang dapat mempengaruhi manajemen likuiditas bank syariah. Beberapa masalah utama yang muncul meliputi serangan ransomware yang mengancam keberlanjutan

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

operasional, risiko pengungkapan data yang dapat merusak kepercayaan nasabah, dan kompleksitas keamanan dalam produk dan layanan syariah. Sementara itu, kekurangan tenaga ahli keamanan siber, perubahan regulasi yang berkembang, dan integrasi teknologi baru menambah kompleksitas manajemen likuiditas dan keamanan. Oleh karena itu, penelitian ini bertujuan untuk merinci dan memahami tantangan-tantangan ini dengan lebih mendalam.

Penelitian akan mengidentifikasi dan menganalisis berbagai jenis serangan siber, seperti ransomware, serta risiko pengungkapan data, dan melihat bagaimana hal ini memengaruhi keberlanjutan manajemen likuiditas. Selain itu Penelitian akan menghasilkan rekomendasi praktis yang dapat membantu bank syariah dalam meningkatkan strategi keamanan siber dan manajemen likuiditas mereka di tengah tantangan yang ada.

Dalam era digital yang semakin maju, perbankan syariah menghadapi transformasi besar dalam pengelolaan likuiditasnya. Manajemen likuiditas yang efektif menjadi krusial untuk menjaga stabilitas keuangan bank syariah, mengingat peran utamanya dalam memastikan ketersediaan dana yang cukup untuk memenuhi kewajiban finansial. Namun, di tengah manfaat teknologi digital, bank syariah juga dihadapkan pada ancaman keamanan siber yang semakin kompleks dan beragam. Oleh karena itu, pemahaman yang mendalam terhadap keamanan siber menjadi aspek yang sangat penting dalam konteks manajemen likuiditas bank syariah di era digital. Perlindungan terhadap data pelanggan; Manajemen likuiditas bank syariah melibatkan pengelolaan data nasabah, termasuk informasi keuangan dan pribadi.

Keamanan siber menjadi kunci untuk melindungi data ini dari potensi serangan yang dapat merugikan integritas dan kerahasiaannya. Keamanan yang tidak memadai dapat mengakibatkan pengungkapan data pelanggan, yang tidak hanya merugikan nasabah tetapi juga dapat merusak reputasi bank. (Vebrianty 2021). Ketergantungan pada transaksi digital ; Bank syariah semakin mengadopsi transaksi digital untuk meningkatkan efisiensi dan memberikan layanan yang lebih baik kepada nasabah. Namun, transaksi digital juga membuka celah bagi serangan siber seperti pencurian identitas, phising, dan malware. Memahami keamanan siber menjadi penting agar transaksi digital bank syariah tetap aman dan dapat diandalkan. (Sriwulan 2023). Integritas dan ketersediaan layanan ; Manajemen likuiditas tidak hanya tentang mencukupi kebutuhan dana, tetapi juga tentang menjaga integritas dan ketersediaan layanan. Serangan siber yang dapat menghentikan atau merusak sistem operasional bank dapat mengganggu proses manajemen likuiditas, mengakibatkan ketidakstabilan finansial dan menurunkan kepercayaan pelanggan.

Kepatuhan terhadap prinsip syariah ; Bank syariah tidak hanya harus mematuhi standar keamanan umum tetapi juga harus memastikan kepatuhan terhadap prinsip-prinsip syariah. Ini mencakup aspek keamanan siber yang melibatkan transparansi, kejujuran, dan perlindungan terhadap nasabah. Pemahaman yang baik terhadap implikasi keamanan siber terhadap prinsip syariah adalah suatu keharusan.Reputasi dan kepercayaan pelanggan ; Keamanan siber dan manajemen likuiditas saling terkait dengan kepercayaan pelanggan. Jika sebuah bank syariah mengalami pelanggaran keamanan siber, hal ini dapat merugikan reputasi bank dan mengurangi kepercayaan pelanggan. Oleh karena itu, memahami keamanan siber menjadi kunci untuk menjaga dan meningkatkan kepercayaan pelanggan dalam manajemen likuiditas bank syariah. (Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki 2022).
Dengan pemahaman yang mendalam terhadap keamanan siber dalam konteks manajemen likuiditas, bank syariah dapat mengambil langkah-langkah proaktif untuk melindungi aset, data, dan reputasi mereka. Ini melibatkan investasi dalam teknologi keamanan canggih, pelatihan karyawan, dan pengembangan kebijakan keamanan yang memadai. Dengan demikian, memahami keamanan siber bukan hanya sebagai tanggung jawab teknologi informasi tetapi sebagai unsur integral dari strategi manajemen likuiditas yang berkelanjutan dan aman di era digital.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Tinjauan Pustaka

Manajemen likuiditas dalam konteks perbankan syariah

a. Prinsip-Prinsip Manajemen Likuiditas dalam Perbankan Syariah
   Literatur terkait manajemen likuiditas dalam konteks perbankan syariah menekankan pentingnya prinsip-prinsip syariah yang memandu pengelolaan likuiditas. Menurut Sundararajan dan Errico (2002), prinsip-prinsip ini mencakup keberlanjutan operasional, ketersediaan dana sesuai dengan prinsip mudharabah, dan pemenuhan kewajiban syariah dalam memastikan bahwa dana dikelola secara adil dan sesuai dengan etika Islam.
b. Keterkaitan Manajemen Likuiditas dan Profitabilitas
   Dalam penelitian oleh (Khan, M.S. and Mirakhor 1987), keterkaitan antara manajemen likuiditas dan profitabilitas dalam perbankan syariah menjadi fokus utama. Mereka menunjukkan bahwa pengelolaan likuiditas yang efektif dapat memberikan kontribusi positif terhadap profitabilitas bank syariah, dengan menciptakan keseimbangan yang optimal antara investasi dan pemenuhan kewajiban finansial.
c. Tantangan Khusus dalam Manajemen Likuiditas Syariah
   Beberapa penelitian, seperti yang dilakukan oleh (Rosly, S. A., & Sanusi 1999), menyoroti tantangan khusus dalam manajemen likuiditas syariah, termasuk kebutuhan untuk mengelola dana tanpa menggunakan instrumen bunga dan mempertimbangkan aspek kepatuhan syariah dalam pengelolaan risiko likuiditas.
d. Instrumen Likuiditas Syariah
   Literatur juga mencakup berbagai instrumen likuiditas syariah yang digunakan oleh bank syariah. Studi oleh (Iqbal, Z., & Mirakhor 2017) mengidentifikasi instrumen seperti wakalah, mudharabah, dan istisna sebagai alat pengelolaan likuiditas yang mematuhi prinsip syariah.
e. Regulasi dan Pengaturan dalam Manajemen Likuiditas Syariah
   Aspek regulasi dan pengaturan dalam manajemen likuiditas syariah turut ditekankan. Menurut (Beck, T., Demirgüç-Kunt, A., & Merrouche 2013), peran regulator dalam menciptakan kerangka kerja yang mendukung manajemen likuiditas syariah sangat vital untuk memastikan kestabilan sektor perbankan syariah secara keseluruhan.
f. Perubahan Teknologi dan Transformasi Digital
   Dengan terus berkembangnya teknologi, literatur terkini menyoroti transformasi digital dan perubahan teknologi yang memengaruhi manajemen likuiditas dalam perbankan syariah. Penelitian oleh (Rahman, M. A., Zaman, N., Asyhari, A. T., Al-Turjman, F., Bhuiyan, M. Z. A., & Zolkipli 2020) menekankan perlunya adaptasi terhadap inovasi digital untuk meningkatkan efisiensi dalam manajemen likuiditas.
g. Dampak Krisis Keuangan Terhadap Manajemen Likuiditas Syariah
   Studi oleh (Mirakhor 2018) menyelidiki dampak krisis keuangan terhadap manajemen likuiditas syariah. Mereka menunjukkan bahwa pengelolaan likuiditas yang efektif dapat menjadi faktor penentu dalam merespons dan mengatasi tantangan yang timbul selama periode ketidakpastian ekonomi.
h. Model Pengukuran Risiko Likuiditas dalam Perbankan Syariah
   Sebagai tambahan, literatur juga mengeksplorasi model pengukuran risiko likuiditas yang khusus untuk perbankan syariah. Penelitian oleh (Abduh 2017) mengembangkan model yang mempertimbangkan karakteristik unik dari perbankan syariah dalam mengidentifikasi dan mengukur risiko likuiditas.

Keamanan siber dalam sektor keuangan dan khususnya di bank syariah

a. Konteks umum keamanan siber di sektor keuangan

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Keamanan siber di sektor keuangan merupakan isu kritis yang terus berkembang seiring dengan kemajuan teknologi. Menurut penelitian oleh (Demchak 2019), sektor keuangan menjadi target utama serangan siber karena menyimpan volume besar data sensitif dan dana nasabah. Keberhasilan operasional dan kepercayaan publik terhadap institusi keuangan sangat bergantung pada keamanan sistem informasi.

b. Ancaman dan serangan terhadap sektor keuangan
Studi oleh (Libicki 2014) mencatat berbagai jenis serangan yang mengintai sektor keuangan, termasuk serangan phishing, malware, dan Distributed Denial of Service (DDoS). Ancaman semacam ini dapat merusak operasional, mencuri data nasabah, dan menyebabkan kerugian finansial yang signifikan. Bank syariah tidak terkecuali dari serangan ini dan perlu mengadopsi strategi keamanan yang canggih.

c. Karakteristik unik keamanan siber di Bank Syariah
Penelitian khusus pada keamanan siber di bank syariah menggarisbawahi karakteristik unik yang membedakan bank syariah dari bank konvensional dalam menghadapi serangan siber. Prinsip syariah yang mengatur transaksi dan pengelolaan dana memerlukan pendekatan keamanan yang mempertimbangkan aspek-etika dan prinsip keadilan dalam pengelolaan risiko siber. (Susanto 2023).

d. Pentingnya kepatuhan terhadap regulasi
Penelitian oleh (Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat 2015) menyoroti pentingnya kepatuhan terhadap regulasi keamanan siber di sektor keuangan. Regulator dan otoritas pengawasan memainkan peran krusial dalam membentuk kerangka kerja keamanan dan memastikan bahwa bank syariah mematuhi standar yang ditetapkan untuk melindungi data dan sistem mereka.

e. Tekhnologi canggih dan keamanan siber di bank syariah
Penerapan teknologi canggih seperti kecerdasan buatan dan analisis big data dalam perbankan syariah juga membawa tantangan dan peluang dalam keamanan siber. Penelitian oleh Agung, I. (Agung, I. G. A., Subhan, M. N., Putri, F. C., & Durya 2023) menekankan perlunya mengintegrasikan teknologi ini dengan strategi keamanan yang adaptif dan responsif terhadap ancaman baru.

f. Pengelolaan identitas dan akses
Dalam literatur keamanan siber di sektor keuangan, pengelolaan identitas dan akses (IAM) memiliki peran yang krusial. Penelitian oleh (Kholis, N., Azra, A., Hasan, N., Qodir, Z., Qibtyah, A., Sadzali, A., & Min Fadhli Robby 2020), menyoroti implementasi IAM yang efektif sebagai salah satu langkah utama dalam melindungi bank syariah dari akses yang tidak sah dan pencurian identitas.

g. Pelibatan pihak ketiga dan resiko keamanan
Pelibatan pihak ketiga, seperti penyedia layanan teknologi keuangan, dapat membuka celah baru untuk serangan siber. Studi oleh (Silalahi 2022), mencatat risiko keamanan yang terkait dengan hubungan dengan pihak ketiga dan menekankan perlunya memastikan bahwa mitra bisnis juga mematuhi standar keamanan yang tinggi.

h. Pendidikan dan kesadaran keamanan
Literatur juga menyoroti pentingnya pendidikan dan kesadaran keamanan di kalangan karyawan bank syariah. Penelitian oleh (Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo 2023), menekankan bahwa pelatihan reguler dan peningkatan kesadaran akan serangan siber dapat menjadi lapisan pertahanan yang kuat dalam menjaga keamanan informasi.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Keterkaitan antara keamanan siber dan stabilitas keuangan

a. Keamanan siber sebagai fondasi stabilitas keuangan
   Keamanan siber diidentifikasi sebagai fondasi utama untuk menjaga stabilitas keuangan dalam sejumlah penelitian. Menurut (Yulianto, A., Utaminingsih, N. S., SE, M., Sari, M. P., & Akt 2023), keamanan siber bukan hanya sebuah isu teknis, tetapi menjadi elemen kritis dalam memelihara kepercayaan publik terhadap lembaga keuangan. Stabilitas keuangan mencakup tidak hanya keberlanjutan operasional, tetapi juga integritas data dan sistem yang menjadi landasan dari operasional tersebut.
b. Dampak serangan siber terhadap stabilitas keuangan
   Penelitian oleh (Gani 2023) menggambarkan dampak serangan siber terhadap stabilitas keuangan sebagai ancaman nyata. Serangan siber yang berhasil dapat mengakibatkan gangguan signifikan pada fungsi operasional lembaga keuangan, memengaruhi integritas data, dan pada akhirnya merusak kepercayaan masyarakat
c. Krisis keuangan dan resiko keamanan siber
   Keterkaitan antara krisis keuangan dan risiko keamanan siber juga dibahas dalam literatur. Menurut (Bacharuddin 2017), kondisi krisis dapat meningkatkan kerentanan terhadap serangan siber karena fokus lebih besar pada pemulihan daripada penguatan keamanan. Oleh karena itu, keterlibatan keamanan siber dalam perencanaan mitigasi risiko menjadi sangat penting
d. Regulasi dan keamanan siber sebagai prioritas utama
   Regulasi yang berkembang memperkuat keterkaitan antara keamanan siber dan stabilitas keuangan. Perlunya kepatuhan lembaga keuangan terhadap kerangka regulasi keamanan siber sebagai salah satu upaya mendukung stabilitas keuangan global. Regulasi ini mendorong lembaga keuangan untuk menginvestasikan sumber daya yang cukup dalam perlindungan terhadap serangan siber. (Ngamal, Y., & Perajaka 2022).
e. Peran keamanan siber dalam mempertahankan kepercayaan publik
   Kepercayaan publik terhadap sektor keuangan sangat terkait dengan keamanan siber. Studi oleh Kegagalan dalam mengelola risiko keamanan siber dapat merusak reputasi lembaga keuangan dan menurunkan tingkat kepercayaan publik, yang pada gilirannya dapat mempengaruhi stabilitas keuangan. (Santoso 2023); (Evi 2023).
f. Hubungan antara keamanan siber dan ketersediaan dana
   Dalam konteks lembaga keuangan, khususnya bank, keamanan siber juga berkaitan erat dengan ketersediaan dana. Menurut (Saputro, E. P., Nasir, M., SE, M., Muhammad Arif, S. E., Setyaningrum, D. P., SE, M., & Febriyanto 2022), serangan siber yang menyebabkan gangguan operasional dapat mengakibatkan penarikan dana masif oleh nasabah yang khawatir, membawa potensi risiko likuiditas dan menggoyahkan stabilitas keuangan.
g. Aspek internasional dan koaborasi dalam keamanan siber
   Studi oleh (Rizal, M., Rukmana, A. Y., Permana, A. A., Fianty, M. I., Saputra, H., Saputri, F. R., ... & Adhicandra 2023) menekankan bahwa keterkaitan antara keamanan siber dan stabilitas keuangan tidak dapat diisolasi secara nasional. Keamanan siber menjadi isu global, dan kerjasama internasional dalam pertukaran informasi dan pelatihan menjadi kunci untuk memitigasi risiko serangan yang dapat berdampak lintas batas.

Metodologi

Penelitian ini akan menggunakan pendekatan studi literatur untuk mendalami dan menganalisis keterkaitan antara keamanan siber dan stabilitas keuangan, khususnya dalam konteks sektor keuangan dan bank syariah. Pendekatan studi literatur dipilih untuk mengidentifikasi temuan-temuan kunci dari penelitian-penelitian sebelumnya, menggambarkan kerangka konseptual yang kokoh, dan menyusun dasar pengetahuan yang mendalam tentang topik ini.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Langkah-langkah metodologi yang akan diambil:

a. **Pemilihan sumber literatur :** Identifikasi sumber literatur melalui basis data akademis, jurnal-jurnal terkemuka, dan publikasi institusi keuangan internasional, Pemilihan literatur yang relevan dengan fokus pada keterkaitan antara keamanan siber dan stabilitas keuangan, dengan penekanan khusus pada sektor keuangan dan bank syariah.
b. **Penetapan kriteria inklusi dan eksklusi :** Menetapkan kriteria inklusi dan eksklusi untuk memastikan bahwa literatur yang digunakan secara langsung relevan dengan topik penelitian, Menyaring literatur berdasarkan kriteria tersebut untuk memastikan keakuratan dan keterkaitan dengan riset ini, Mengadakan analisis mendalam terhadap temuan-temuan kunci dari literatur terpilih, Mengidentifikasi pola dan tren yang muncul dalam hubungan antara keamanan siber dan stabilitas keuangan.
c. **Pembentukan kerangka konseptual :** Membentuk kerangka konseptual yang menggambarkan keterkaitan antara keamanan siber dan stabilitas keuangan, dengan memperhitungkan elemen-elemen kunci yang diidentifikasi dari literatur.
d. **Identifikasi kesenjangan pengetahuan** dengan Mengidentifikasi kesenjangan dalam pengetahuan yang mungkin muncul dari literatur yang telah diulas, Menentukan area-area penelitian lanjutan yang dapat dijelajahi berdasarkan temuan literatur yang ada.

Sumber data dan teknik pengumpulan data

a. Jurnal dan publikasi akademik : Menggunakan sumber data dari jurnal ilmiah terkemuka dalam bidang keamanan siber, keuangan, dan bank syariah. Sumber ini akan menyediakan tinjauan literatur mendalam dan hasil penelitian terkini.
b. Buku rujukan dan monograf :Mengacu pada buku-buku khusus yang memberikan landasan teoretis dan konseptual yang mendukung penelitian. Buku-buku ini dapat mencakup aspek keamanan siber, stabilitas keuangan, dan konteks bank syariah.
c. Laporan dan publikasi institusi keuangan :Mengumpulkan data dan informasi dari laporan dan publikasi yang diterbitkan oleh lembaga-lembaga keuangan internasional seperti IMF, World Bank, dan Bank for International Settlements (BIS).

Teknik Pengumpulan Data:

a. **Pencarian dan analisis literatur** : Melakukan pencarian intensif dalam basis data akademis seperti *PubMed, IEEE Xplore, dan Google Scholar* untuk mengidentifikasi jurnal dan artikel terkait, Menerapkan teknik analisis literatur untuk mengevaluasi dan mensintesis temuan-temuan kunci dari literatur yang ditemukan.
b. **Studi dokumen dan analisis regulasi** : Melakukan studi dokumen terhadap laporan, panduan, dan regulasi terkait keamanan siber dalam sektor keuangan, Menganalisis dokumen-dokumen ini untuk memahami pendekatan dan langkah-langkah yang telah diambil untuk menjaga stabilitas keuangan.

Kerangka analisis : Kerangka analisis ini dirancang untuk menyelidiki dan menganalisis keterkaitan antara keamanan siber dan stabilitas keuangan dalam konteks sektor keuangan, khususnya di bank syariah. Kerangka analisis ini terdiri dari beberapa dimensi utama yang mencakup literatur, regulasi, praktik industri, dan dampak serangan siber terhadap stabilitas keuangan.

literatur terkait:

a. Keamanan siber dalam sektor keuangan
   Mengumpulkan temuan-temuan kunci dari literatur terkait keamanan siber dalam sektor keuangan, termasuk definisi konsep, jenis serangan yang umum, dan strategi pengamanan yang diterapkan
b. Stabilitas keuangan

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Meninjau literatur yang memperjelas konsep stabilitas keuangan, faktor-faktor yang mempengaruhinya, dan indikator-indikator yang digunakan untuk mengukur stabilitas keuangan.

c. Keterkaitan dan studi terdahulu
Menganalisis penelitian-penelitian sebelumnya yang telah mengeksplorasi hubungan antara keamanan siber dan stabilitas keuangan, mencatat metodologi dan temuan utama.

Regulasi dan kebijakan

a. Regulasi keamanan siber
Mengidentifikasi dan menganalisis regulasi yang berlaku terkait keamanan siber dalam sektor keuangan, terutama di konteks bank syariah

b. Kebijakan stabilitas keuangan
Meninjau kebijakan-kebijakan yang diterapkan oleh regulator untuk menjaga stabilitas keuangan, khususnya yang berkaitan dengan keamanan siber

Praktek keamanan siber di Bank Syariah

Mengumpulkan informasi tentang praktik keamanan siber yang umum diterapkan oleh bank syariah, termasuk teknologi dan strategi yang digunakan

Hasil dan Pembahasan

Hasil Pembahasan temuan dan implikasinya terhadap praktik manajemen likuiditas dan keamanan siber

Hasil Pembahasan penelitian mengenai manajemen likuiditas dan keamanan siber pada bank syariah memberikan wawasan yang mendalam terhadap bagaimana hasil penelitian dapat diterapkan dalam praktik manajemen likuiditas dan keamanan siber. Berikut adalah penjelasan mengenai pembahasan temuan dan implikasinya terhadap praktik kedua aspek tersebut:

a. Manajemen Likuiditas
Analisis menunjukkan bahwa penerapan strategi manajemen likuiditas yang lebih proaktif dapat membantu bank syariah menghadapi fluktuasi likuiditas dengan lebih efektif. Bank syariah dapat mempertimbangkan diversifikasi sumber likuiditas, meningkatkan monitoring terhadap aliran kas, dan mengembangkan skenario stres yang lebih realistis. Meminimalkan risiko ketidakmampuan memenuhi kewajiban pembayaran, meningkatkan efisiensi pengelolaan likuiditas, dan mendukung keberlanjutan operasional.

b. Keamanan Siber
Temuan penelitian menunjukkan bahwa ketidakpahaman karyawan terhadap risiko keamanan siber menjadi faktor utama rentannya bank syariah terhadap serangan siber. Pelatihan secara teratur dan peningkatan kesadaran keamanan di kalangan karyawan perlu diperkuat untuk mengurangi risiko serangan sosial teknik dan kebocoran informasi. Meningkatkan ketahanan terhadap serangan siber, mengurangi peluang serangan dari dalam, dan meningkatkan respons cepat terhadap ancaman keamanan.

c. Integrasi manajemen likuiditas dan keamanan siber
Integrasi strategi manajemen likuiditas dengan keamanan siber menjadi kunci dalam memastikan stabilitas keuangan dan keamanan bank syariah. Perlu ada kolaborasi erat antara divisi manajemen likuiditas dan keamanan siber untuk mengidentifikasi dan mengatasi potensi risiko yang berkaitan. Meningkatkan efisiensi operasional, meminimalkan risiko serangan yang dapat mempengaruhi likuiditas, dan menciptakan lingkungan keamanan yang holistik.

d. Keterkaitan dengan prinsip syariah
Prinsip syariah dapat mempengaruhi strategi manajemen likuiditas dan keamanan siber, terutama dalam konteks kepatuhan terhadap nilai-nilai etika Islam. Strategi yang diadopsi harus sesuai dengan prinsip-prinsip syariah, dan penilaian dampak terhadap kepatuhan syariah

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

perlu menjadi pertimbangan utama. Mempertahankan integritas bank syariah, meningkatkan kepercayaan nasabah, dan menjaga reputasi sebagai lembaga keuangan yang patuh syariah.

e. Penerapan tekhnologi dan inovasi
Penerapan teknologi canggih dan inovasi dalam manajemen likuiditas dan keamanan siber dapat meningkatkan daya saing bank syariah. Investasi dalam teknologi terbaru dan kebijakan inovatif dapat meningkatkan efisiensi, meminimalkan risiko, dan memberikan pengalaman nasabah yang lebih aman. Meningkatkan daya saing di pasar, memikat nasabah yang semakin cerdas teknologi, dan memberikan keunggulan dalam menghadapi ancaman siber yang semakin kompleks.

Hasil Pembahasan temuan dan implikasinya terhadap praktik manajemen likuiditas dan keamanan siber memberikan panduan praktis bagi bank syariah dalam meningkatkan kinerja operasional dan menjaga keamanan serta stabilitas keuangan. Integrasi strategi, kesadaran syariah, dan penerapan teknologi menjadi kunci untuk mencapai keberhasilan dalam dua aspek yang krusial ini. Dengan mengambil langkah-langkah ini, bank syariah dapat memastikan kesinambungan operasional yang berkelanjutan dan tetap memegang teguh prinsip-prinsip etika Islam dalam praktik bisnisnya

Pembahasan

Analisis mendalam hasil penelitian

Bank syariah, seperti lembaga keuangan lainnya, menghadapi sejumlah tantangan serius terkait dengan keamanan siber di era digital yang terus berkembang. Analisis mendalam terhadap tantangan ini membuka wawasan tentang kompleksitas dan signifikansinya dalam mempertahankan stabilitas keuangan dan kepercayaan publik. Berikut adalah tinjauan rinci terhadap beberapa tantangan keamanan siber utama yang dihadapi oleh bank syariah:

a. Serangan phising and social engineering : Bank syariah rentan terhadap serangan phishing yang menggunakan teknik manipulasi psikologis untuk memperoleh informasi rahasia dari nasabah atau karyawan. Keberhasilan serangan phishing dapat merusak reputasi bank syariah dan menyebabkan kehilangan dana nasabah.

b. **Malware dan Ransomware :** Ancaman malware dan ransomware dapat mengakibatkan kebocoran data, pencurian informasi keuangan, atau penguncian sistem yang dapat mengganggu operasional bank, Kehilangan kontrol terhadap sistem dan data sensitif, serta potensi untuk membayar tebusan dalam serangan ransomware

c. **Tantangan kepatuhan syariah :**Menjaga keamanan siber sekaligus mematuhi prinsip-prinsip syariah menjadi tantangan unik bagi bank syariah, yang harus memastikan kepatuhan terhadap norma dan etika Islam. Pelanggaran prinsip syariah dapat merusak citra bank syariah dan mengancam stabilitas keuangan yang didasarkan pada kepercayaan nasabah.

d. **Ketidakpastian hukum dan regulasi :**Lingkungan regulasi yang terus berubah dapat membuat sulit bagi bank syariah untuk mengikuti standar keamanan siber yang relevan. Keterlambatan dalam mematuhi regulasi dapat berakibat pada sanksi hukum dan reputasi yang merugikan.

e. **Kurangnya kesadaran keamanan :** Baik dari pihak internal maupun eksternal, kurangnya kesadaran tentang risiko keamanan siber dapat meningkatkan kemungkinan terjadinya pelanggaran keamanan. Karyawan dan nasabah yang tidak teredukasi dapat menjadi pintu masuk bagi serangan, meningkatkan risiko kerentanan keamanan.

f. **Pengelolaan identitas dan akses yang tidak efektif :** Pengelolaan identitas dan akses yang tidak efektif dapat memberikan peluang bagi pihak tidak berwenang untuk mengakses sistem dan data kritis. Risiko pencurian identitas, penipuan, dan akses tidak sah ke dana nasabah atau informasi rahasia bank.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

g. **Tantangan tekhnologi finansial :** Penyedia layanan finansial teknologi yang pesat dapat membawa tantangan baru dalam hal keamanan siber, karena bank syariah harus berintegrasi dengan teknologi ini. Risiko terhadap keamanan data dan integrasi yang tidak aman dengan solusi fintech dapat merusak reputasi dan kepercayaan nasabah.

Analisis ini menggarisbawahi kompleksitas tantangan keamanan siber yang dihadapi oleh bank syariah. Melibatkan berbagai aspek seperti teknologi, regulasi, dan kepatuhan syariah, penanganan tantangan ini memerlukan pendekatan holistik yang mencakup pendidikan keamanan, kebijakan yang kuat, dan investasi dalam teknologi canggih untuk melindungi stabilitas keuangan dan kepercayaan nasabah.

Kesimpulan

Dalam rangka memahami kompleksitas manajemen likuiditas dan keamanan siber pada bank syariah, penelitian ini telah menghasilkan temuan-temuan kunci yang memberikan wawasan mendalam. Ringkasan temuan utama dapat disajikan sebagai berikut:

a. Manajemen Likuiditas:
   - Ditemukan bahwa diversifikasi sumber likuiditas menjadi faktor krusial dalam meningkatkan ketahanan bank syariah terhadap fluktuasi likuiditas.
   - Temuan menunjukkan bahwa pengelolaan aliran kas yang efektif membantu bank syariah menghindari risiko tidak likuiditas dan mendukung operasional yang lancar.
   - Strategi manajemen likuiditas yang proaktif memberikan keuntungan dalam mengatasi tantangan likuiditas yang muncul secara mendadak.

b. Keamanan Siber:
   - Ditemukan bahwa ketidakpahaman karyawan terhadap risiko keamanan siber menjadi faktor utama rentannya bank syariah terhadap serangan.
   - Kesimpulan menunjukkan bahwa pelatihan dan peningkatan kesadaran keamanan di kalangan karyawan dapat mengurangi risiko serangan siber yang melibatkan faktor manusia.
   - Prinsip syariah perlu diintegrasikan dalam strategi keamanan siber untuk memastikan kepatuhan dan kepercayaan nasabah.

c. Integrasi Manajemen Likuiditas dan Keamanan Siber:
   - Kesimpulan menggarisbawahi bahwa kolaborasi erat antara divisi manajemen likuiditas dan keamanan siber adalah kunci untuk mengidentifikasi dan mengatasi potensi risiko yang berkaitan.
   - Integrasi teknologi canggih dan inovasi dalam kedua aspek ini memberikan keunggulan kompetitif dan meningkatkan ketahanan terhadap tantangan modern.
   - Kesimpulan menegaskan bahwa penerapan strategi harus selaras dengan prinsip-prinsip syariah untuk memastikan integritas bank syariah.

Ringkasan temuan utama ini memberikan dasar bagi bank syariah untuk memperkuat praktik manajemen likuiditas dan keamanan siber mereka. Dengan memahami tantangan, penerapan strategi yang efektif, dan mempertimbangkan prinsip-prinsip syariah, bank syariah dapat memastikan keberlanjutan operasional dan menjaga kepercayaan nasabah dalam menghadapi lingkungan bisnis yang dinamis dan penuh risiko.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Implikasi praktis dan rekomendasi untuk penelitian lebih lanjut

a. Implikasi praktis
   1. Bank syariah dapat mengoptimalkan manajemen likuiditas dengan diversifikasi sumber likuiditas, termasuk menjalin kerja sama dengan lembaga keuangan lain dan memanfaatkan instrumen keuangan yang sesuai dengan prinsip syariah.
   2. Implementasi program pelatihan reguler dan peningkatan kesadaran keamanan di kalangan karyawan dapat dilakukan untuk memitigasi risiko serangan siber yang melibatkan faktor manusia
   3. Bank syariah dapat memperkuat integrasi antara divisi manajemen likuiditas dan keamanan siber melalui forum kolaboratif, pertukaran informasi terstruktur, dan pengembangan kebijakan terintegrasi
   4. Bank syariah dapat memanfaatkan teknologi canggih dan inovasi, termasuk implementasi kecerdasan buatan dan analisis big data, untuk meningkatkan keamanan siber dan efisiensi manajemen likuiditas
   5. Keberlanjutan bank syariah dapat diperkuat dengan memprioritaskan kesadaran syariah dalam strategi manajemen likuiditas dan keamanan siber.

b. Rekomendasi untuk penelitian lebih lanjut
   1. Penelitian lebih lanjut dapat dilakukan untuk menganalisis dampak teknologi finansial (FinTech) terhadap manajemen likuiditas dan keamanan siber di bank syariah, serta strategi adaptasi yang dapat diterapkan
   2. Penelitian dapat mengeksplorasi peran teknologi blockchain dalam meningkatkan transparansi dan efisiensi dalam manajemen likuiditas bank syariah
   3. Penelitian lebih lanjut dapat dilakukan untuk menganalisis tingkat kesiapan keamanan siber di bank syariah, termasuk evaluasi terhadap infrastruktur teknologi dan kebijakan keamanan yang diterapkan
   4. Penelitian dapat mengeksplorasi pengaruh faktor eksternal, seperti perubahan regulasi atau kondisi pasar global, terhadap manajemen likuiditas bank syariah
   5. Penelitian dapat mengembangkan model prediktif risiko keamanan siber yang memanfaatkan kecerdasan buatan untuk mendeteksi dan mencegah serangan secara proaktif
   6. Studi kasus tentang penerapan terbaik dalam manajemen likuiditas dan keamanan siber di bank syariah dapat memberikan wawasan praktis untuk lembaga serupa

Referensi

Abduh, M. 2017. “Competitive Condition and Market Power of Islamic Banks in Indonesia.” *International Journal of Islamic and Middle Eastern Finance and Management* 20 (1): 77–91.

Abdul, A. R., Mandiri, D. P., Astuti, W., & Arkoyah, S. 2022. “Tantangan Perkembangan Perbankan Syariah Di Indonesia.” *Jurnal Tabarru’: Islamic Banking and Finance* 5 (2): 352–65.

Agung, I. G. A., Subhan, M. N., Putri, F. C., & Durya, N. P. M. A. 2023. “Manajemen Keuangan Menghadapi Industri 5.0.” *Cendikia Mulia Mandiri* 2 (1): 22–32.

Bacharuddin, M. A. 2017. “The Impact of Macroeconomic Variables towards Economic Growth in Malaysia.” *Journal of Education Technology*.

Beck, T., Demirgüç-Kunt, A., & Merrouche, O. 2013. “Islamic vs. Conventional Banking: Business Model, Efficiency and Stability.” *Journal of Banking & Finance* 37 (2): 433–47.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. 2015. “Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources.” *Information & Management* 52 (3): 385–400.

Demchak, C. C. 2019. “China: Determined to Dominate Cyberspace and AI.” *Bulletin of the Atomic Scientists* 75 (3): 99–104.

Evi, T. 2023. “Transformasi Transaksi Tunai Ke Digital Di Indonesia.”

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & 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.

krigan :
Krigan: Journal of Management and Sharia Business
http://dx.doi.org/10.30983/krigan.v1i2.7929
Vol. 1. No. 2 Edisi Juli – Desember 2023

Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki, S. N. 2022. *Fintech Dalam Keuangan Islam: Teori Dan Praktik*.

Gani, T. A. 2023. "Kedaulatan Data Digital Untuk Integritas Bangsa." *Yiah Kuala University Press.*

Iqbal, Z., & Mirakhor, A. 2017. "Ethical Dimensions of Islamic Finance: Theory and Practice." *Springer*.

Khan, M.S. and Mirakhor, A. 1987. "The Financial System and Monetary Policy in an Islamic Economy." *Ln Theoretical Studies in Islamic Banking and Finance*.

Kholis, N., Azra, A., Hasan, N., Qodir, Z., Qibtyah, A., Sadzali, A., & Min Fadhli Robby, H. 2020. "Islam Indonesia 2020."

Libicki, Ablon. 2014. "Ancaman Dan Serangan Terhadap Sektor Keuangan." *Jurnal Sains Dan Informatika*.

Mirakhor, Haque. 2018. "Dampak Krisis Keuangan Terhadap Manajemen Likuiditas Syariah." *Manajemen*.

Munawarah, H., Yusuf, M., & Komarudin, P. 2022. "Bank digital syariah: analisis cyber security menurut hukum positif di indonesia dan hukum ekonomi syariah."

Ngamal, Y., & Perajaka, M. A. 2022. "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia." *Jurnal Manajemen Risiko* 2 (2): 59–75.

Raharjo, B. 2021. "Fintech Teknologi Finansial Perbankan Digital." *Penerbit Yayasan Prima Agus Teknik*, 1–299.

Rahman, M. A., Zaman, N., Asyhari, A. T., Al-Turjman, F., Bhuiyan, M. Z. A., & Zolkipli, M. F. 2020. "Ata-Driven Dynamic Clustering Framework for Mitigating the Adverse Economic Impact of Covid-19 Lockdown Practices." *Sustainable Cities and Society* 2: 10–23.

Rizal, M., Rukmana, A. Y., Permana, A. A., Fianty, M. I., Saputra, H., Saputri, F. R., ... & Adhicandra, I. 2023. "Transformasi Digital: Memahami Internet Of Things." *Get Press Indonesia*.

Rosly, S. A., & Sanusi, M. M. 1999. "He Application of Bay'al-'inah and Bay'al-Dayn in Malaysian Islamic Bonds–an Islamic Analysis." *International Journal of Islamic Financial Services* 1 (2): 3–11.

Santoso, J. T. 2023. *Teknologi Keamanan Siber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik.

Saputro, E. P., Nasir, M., SE, M., Muhammad Arif, S. E., Setyaningrum, D. P., SE, M., & Febriyanto, A. 2022. "Digitalisasi Perbankan: Prospek, Tantangan & Kinerja." *Muhammadiyah University Press.*

Silalahi, F. D. 2022. *Keamanan Cyber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik.

SRIWULAN, S. 2023. "Tinjauan Yuridis Tindak Pidana Cyber Crime Di Indonesia (Doctoral Dissertation." *Institut Agama Islam Negeri Palopo).*

Susanto, D. 2023. *Etika bisnis*. tohar media.

vebrianty, a. 2021. "perlindungan hukum pembukaan rekening secara online dalam layanan perbankan digital pada pt bank central asia Tbk (Bachelor's Thesis." *Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta).*

Yulianto, A., Utaminingsih, N. S., SE, M., Sari, M. P., & Akt, C. A. 2023. *Sistem Informasi Manajemen.* Cahya Ghani Recovery.