Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI

Muhazzab Alief Faizal[1], Zelyn Faizatul[2], Binti Nur Asiyah[3], Rokhmat Subagyo[4],

[1]Ekonomi Syariah, Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung
[2]Ekonomi Syariah, Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung
[3]Ekonomi Syariah, Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung
[41]Ekonomi Syariah, Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung
E-mail: muhazzab.29@gmail.com

Abstrak

Artikel ini membahas analisis risiko teknologi informasi pada bank syariah dan mengidentifikasi ancaman serta tantangan terkini yang dihadapi oleh industri perbankan dalam menjaga keamanan sistem. Metode yang digunakan adalah studi literatur dengan analisis sumber informasi terpercaya yang relevan. Metode ini digunakan untukmengumpulkan data dan informasi terkait risiko keamanan yang dihadapi oleh bank syariah. Hasil pembahasan menunjukkan bahwa bank syariah menghadapi ancaman terkini signifikan, seperti kejahatan siber, serangan malware dan ransomware, phising, social engineering, pelanggaran data, serta pencurian identitas. Ancaman ini berpotensi merusak sistem perbankan dan melanggar privasi nasabah. Tantangan dalam menghadapi ancaman terkini meliputi evolusi serangan yang semakin kompleks, kurangnya kesadaran dan keterampilan keamanan pada pengguna, serta perubahan regulasi dan kebijakan. Implementasi sistem keamanan yang tepat dianjurkan, termasuk identifikasi risiko komprehensif, penggunaan teknologi keamanan mutakhir, pengawasan dan pemantauan aktif, serta pelatihan dan kesadaran keamanan yang terus-menerus. Implementasi kebijakan keamanan yang jelas dan terdokumentasi, evaluasi dan pengujian keamanan yang teratur, serta pematuhan terhadap regulasi dan kebijakan privasi juga penting. Artikel ini menjelaskan pentingnya menjaga keamanan teknologi informasi dan menekankan perlunya implementasi sistem keamanan yang tepat, kolaborasi dengan lembaga keamanan siber, serta pembaruan teknologi keamanan yang berkelanjutan untuk mengurangi risiko serangan dan melindungi sistem dan informasi nasabah dengan lebih efektif.

Kata Kunci: *: risiko teknologi informasi, bank syariah, keamanan sistem, ancaman terkini, studi literatur.*

1. Pendahuluan

Dalam era digital yang terus berkembang, sektor perbankan tidak terkecuali menghadapi tantangan baru dalam mengelola risiko teknologi informasi. Teknologi informasi memainkan peran yang sangat penting dalam operasional bank syariah modern, mulai dari sistem perbankan online hingga aplikasi perbankan seluler. Namun, bersamaan dengan keuntungan yang ditawarkan oleh kemajuan teknologi ini, bank syariah juga dihadapkan pada berbagai ancaman dan tantangan yang signifikan.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Bank syariah memiliki kekhasan dalam prinsip-prinsipnya yang didasarkan pada syariat Islam, termasuk dalam pengelolaan risiko. Mereka dituntut untuk menjaga kerahasiaan, integritas, dan ketersediaan data nasabah dengan memastikan implementasi teknologi informasi yang aman dan sesuai dengan prinsip syariah. Ancaman terhadap keamanan dan privasi informasi nasabah semakin meningkat, dengan peningkatan serangan siber dan perkembangan teknik kejahatan yang semakin canggih. (Ariffin, 2014)

Dunia terus mengalami perubahan sesuai dengan perkembangan zaman. Negara maju maupun negara berkembang terus menunjukkan perubahan dan perkembangannya, seperti di indonesia. Perkembangan tersebut dapat di lihat dari segi teknologi, pembangunan, maupun industri. (Mulya, 2021)

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. Seiring dengan kemajuan teknologi, bank syariah menggunakan sistem perbankan online, aplikasi perbankan seluler, dan layanan digital lainnya untuk memenuhi kebutuhan nasabah secara efisien. Namun, bersamaan dengan manfaat yang ditawarkan oleh teknologi ini, juga muncul ancaman dan tantangan yang signifikan dalam menjaga keamanan informasi dan mengelola risiko teknologi informasi dengan benar.

Bank syariah bertanggung jawab untuk melindungi data nasabah dan menjaga kerahasiaan serta integritas informasi. Namun, ancaman terhadap keamanan informasi semakin kompleks dan berkembang seiring waktu. Serangan siber yang dilakukan oleh peretas yang mahir semakin terorganisir dan sofistikasi, mengancam kerahasiaan data nasabah, keutuhan sistem, dan ketersediaan layanan. Kejahatan siber seperti phishing, serangan malware, dan pencurian identitas menjadi ancaman yang serius bagi bank syariah. (Bruce, 2015)

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.

Dalam konteks ini, analisis risiko teknologi informasi menjadi sangat penting untuk bank syariah. Identifikasi ancaman dan tantangan terkini dalam teknologi informasi dapat membantu bank syariah dalam merancang strategi keamanan yang efektif dan mencegah kerugian yang tidak diinginkan. Penting untuk memahami tren ancaman terbaru dalam teknologi informasi, serta tantangan yang dihadapi dalam menghadapi ancaman tersebut.

Penelitian yang menyeluruh dan pemahaman yang mendalam tentang risiko teknologi informasi pada bank syariah diperlukan untuk membantu mengembangkan strategi pengamanan yang tepat. Studi literatur menyediakan sumber informasi yang berharga dalam menganalisis risiko teknologi informasi dan mengidentifikasi ancaman serta tantangan terkini dalam konteks bank syariah. Melalui pendekatan studi literatur, data dan informasi yang relevan tentang risiko teknologi informasi pada bank syariah dapat dikumpulkan, dianalisis, dan dievaluasi secara komprehensif. (Corne, 2020)

Penelitian ini bertujuan untuk menganalisis risiko teknologi informasi pada bank syariah, dengan fokus pada identifikasi ancaman dan tantangan terkini. Dengan melibatkan studi literatur yang luas, artikel ini akan menggali dan mengevaluasi literatur terkait yang telah dipublikasikan dalam bidang risiko teknologi informasi pada bank syariah. Data dan informasi yang dikumpulkan dari studi literatur akan digunakan untuk mengidentifikasi

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

ancaman terkini dalam teknologi informasi pada bank syariah serta tantangan yang harus dihadapi dalam menghadapi ancaman tersebut.

Dengan demikian, artikel ini diharapkan dapat memberikan pemahaman yang lebih baik tentang risiko teknologi informasi dalam konteks bank syariah dan memberikan wawasan yang berharga tentang strategi pengamanan yang diperlukan untuk menghadapi ancaman dan tantangan terkini.

2. Metode Penelitian

Metodologi penelitian yang digunakan dalam artikel ini melibatkan pengumpulan data melalui studi literatur yang komprehensif. Melalui pendekatan ini, informasi yang relevan tentang risiko teknologi informasi pada bank syariah dapat dikumpulkan, dianalisis, dan dievaluasi secara sistematis. Pengumpulan data dalam penelitian ini dilakukan melalui studi literatur yang melibatkan pencarian dan analisis berbagai referensi terkait risiko teknologi informasi pada bank syariah. Sumber data yang digunakan meliputi jurnal ilmiah, buku, makalah konferensi, dan dokumen terkait lainnya. Melalui penggunaan sumber data yang beragam, penelitian ini bertujuan untuk mendapatkan pemahaman yang komprehensif tentang ancaman dan tantangan terkini dalam teknologi informasi pada bank syariah.

Sumber data yang digunakan dalam penelitian ini meliputi literatur terkait yang telah dipublikasikan dalam bidang risiko teknologi informasi pada bank syariah. Jurnal ilmiah yang terkait dengan manajemen risiko teknologi informasi, keamanan informasi, kejahatan siber, dan prinsip syariah dalam perbankan syariah menjadi sumber utama untuk memperoleh informasi yang akurat dan berwawasan luas. Selain itu, buku dan makalah konferensi juga digunakan untuk memperkaya pemahaman tentang risiko teknologi informasi pada bank syariah. Dalam memilih literatur yang relevan, kriteria tertentu digunakan untuk memastikan kualitas dan keakuratan informasi yang diperoleh. Pertama, literatur yang dipilih harus terkait dengan risiko teknologi informasi pada bank syariah. Fokus utama adalah pada identifikasi ancaman dan tantangan terkini dalam teknologi informasi yang dihadapi oleh bank syariah. Kedua, literatur yang digunakan harus bersifat ilmiah dan telah melalui proses peer review, sehingga dapat diandalkan dalam memberikan informasi yang akurat dan berbasis bukti. Ketiga, literatur yang diperoleh harus merupakan sumber yang mutakhir, termasuk publikasi dalam kurun waktu yang relevan dengan penelitian ini.

Validitas studi literatur dalam penelitian ini sangat penting untuk memastikan kualitas dan keandalan data yang digunakan. Untuk menjamin validitas studi literatur, langkah-langkah berikut diambil. Pertama, penggunaan sumber literatur yang terpercaya dan berkualitas, seperti jurnal ilmiah yang diindeks dan buku dari penerbit terkemuka. Kedua, kritikalitas dan analisis yang hati-hati dilakukan dalam memilih literatur yang relevan dan sesuai dengan tujuan penelitian. Ketiga, proses seleksi literatur yang transparan dan dapat direplikasi, dengan mempertimbangkan kriteria yang telah ditetapkan sebelumnya. Dengan pendekatan yang didasarkan pada studi literatur dan memperhatikan validitas penelitian, artikel ini bertujuan untuk menyajikan informasi yang terpercaya dan berbasis bukti tentang risiko teknologi informasi pada bank syariah, dengan fokus pada identifikasi ancaman dan tantangan terkini.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

3. Hasil dan Pembahasan

3.1. Ancaman Terkini dalam Teknologi Informasi pada Bank Syariah

Bank syariah saat ini menghadapi ancaman yang semakin kompleks dalam penggunaan teknologi informasi. Ancaman ini meliputi serangan siber yang dilakukan oleh peretas yang mahir, pelanggaran privasi data, dan pelanggaran terhadap prinsip syariah dalam pengelolaan informasi keuangan. Dalam konteks ini, pemahaman yang mendalam tentang ancaman terkini dalam teknologi informasi pada bank syariah menjadi penting dalam upaya melindungi keamanan informasi dan menjaga kepercayaan nasabah. (Cremer, 2022)

Salah satu ancaman terkini adalah serangan siber yang dilakukan oleh peretas yang mahir. Peretas dapat menggunakan berbagai metode seperti phishing, serangan malware, dan pencurian identitas untuk mengakses data nasabah dan merusak sistem perbankan. Serangan phishing melibatkan penipuan melalui email atau situs web palsu yang mengecoh nasabah untuk mengungkapkan informasi pribadi atau keuangan. Serangan malware, seperti ransomware, dapat menginfeksi sistem dan mengenkripsi data sehingga nasabah atau bank harus membayar tebusan untuk mendapatkan akses kembali. Pencurian identitas juga menjadi ancaman serius, di mana peretas mencuri identitas nasabah dan menggunakannya untuk melakukan kegiatan ilegal atau penipuan. (Sanchez et all (2018)

Ancaman lain yang dihadapi oleh bank syariah adalah pelanggaran privasi data. Dalam era digital, data nasabah menjadi aset berharga yang harus dilindungi. Pelanggaran privasi data dapat mengakibatkan kerugian finansial dan kerugian reputasi yang signifikan bagi bank syariah. Ancaman ini dapat berasal dari serangan siber atau dari insiden internal seperti kebocoran data atau akses yang tidak sah oleh karyawan yang tidak bertanggung jawab. Keberhasilan menjaga privasi data nasabah menjadi kunci dalam mempertahankan kepercayaan dan loyalitas nasabah.

Selain itu, bank syariah juga menghadapi tantangan dalam mematuhi prinsip syariah dalam pengelolaan informasi keuangan. Bank syariah harus memastikan bahwa teknologi yang mereka gunakan sesuai dengan prinsip-prinsip syariah, seperti larangan riba dan transaksi yang tidak sesuai dengan hukum Islam. Tantangan ini melibatkan pengawasan dan pengendalian yang ketat terhadap sistem perbankan online dan aplikasi perbankan seluler untuk memastikan bahwa semua transaksi dan operasi sesuai dengan prinsip syariah.

Untuk menghadapi ancaman dan tantangan tersebut, bank syariah perlu mengadopsi strategi keamanan yang komprehensif. Hal ini meliputi penerapan langkah-langkah keamanan yang kuat seperti enkripsi data, pemantauan jaringan yang terus-menerus, pelatihan keamanan bagi karyawan, dan audit keamanan secara berkala. Selain itu, kerja sama dengan lembaga keamanan dan regulator juga penting dalam membangun kerangka kerja yang efektif dalam menghadapi ancaman teknologi informasi. Selain itu beberapa anacaman meliputi beberapa point yang akan dijelaskan sebagai beirkut :

a) Kejahatan Siber

Kejahatan siber telah menjadi ancaman yang semakin meningkat dalam era digital saat ini. Dalam konteks teknologi informasi pada bank syariah, 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, seperti pencurian data, serangan peretasan, penipuan online, dan penyebaran malware. Pemahaman yang mendalam tentang jenis-jenis kejahatan siber ini menjadi penting dalam upaya melindungi sistem perbankan syariah dan menjaga integritas informasi keuangan. (Jakobsson, 2020)

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Salah satu bentuk kejahatan siber yang umum adalah pencurian data. Pencurian data dapat terjadi melalui serangan siber yang ditujukan untuk mendapatkan akses tidak sah ke informasi sensitif seperti nomor kartu kredit, data keuangan, dan informasi pribadi nasabah. Data yang dicuri kemudian dapat digunakan untuk tujuan penipuan, identitas palsu, atau dijual kepada pihak ketiga yang tidak bertanggung jawab. Pencurian data dapat merusak reputasi bank syariah dan mengakibatkan kerugian finansial bagi nasabah yang menjadi korban.

Serangan peretasan juga menjadi ancaman serius dalam kejahatan siber. Peretas menggunakan keahlian teknis mereka untuk meretas sistem perbankan dan mendapatkan akses tidak sah ke data dan informasi sensitif. Serangan peretasan dapat mengakibatkan kerugian yang signifikan, termasuk pencurian dana, manipulasi transaksi, dan merusak infrastruktur teknologi bank. Peretasan yang sukses dapat merusak reputasi bank syariah dan mengganggu layanan perbankan yang penting bagi nasabah.

Selain itu, penipuan online juga merupakan bentuk kejahatan siber yang umum. Penipuan online melibatkan praktik penipuan yang menggunakan teknologi informasi, seperti phishing, scam, atau penjualan barang palsu secara online. Penipuan online sering kali menargetkan nasabah bank dan mencoba memperoleh informasi pribadi, kata sandi, atau data keuangan mereka. Penipuan online dapat merusak kepercayaan nasabah dan menyebabkan kerugian finansial yang signifikan. Kshetri (2010)

Untuk mengatasi kejahatan siber, bank syariah harus mengadopsi langkah-langkah keamanan yang proaktif. Ini meliputi investasi dalam sistem keamanan yang canggih, pelatihan keamanan bagi karyawan, pemantauan jaringan yang ketat, dan kerja sama dengan lembaga keamanan dan penegak hukum. Penting bagi bank syariah untuk memperbarui dan memperkuat kebijakan keamanan mereka secara teratur, termasuk kebijakan sandi yang kuat, pembaruan perangkat lunak yang teratur, dan enkripsi data yang kuat. Selain itu, pendidikan dan kesadaran nasabah juga menjadi faktor penting dalam melawan kejahatan siber. Bank syariah dapat memberikan edukasi kepada nasabah tentang praktik keamanan online, pentingnya melindungi informasi pribadi, dan bagaimana mengenali tanda-tanda penipuan online.

Selain langkah-langkah keamanan teknis, kerja sama dengan lembaga keamanan dan penegak hukum juga penting dalam menghadapi kejahatan siber. Bank syariah dapat bekerja sama dengan lembaga keamanan siber untuk mendapatkan informasi tentang ancaman terkini dan mengidentifikasi celah keamanan yang mungkin ada dalam sistem mereka. Selain itu, jika terjadi kejahatan siber, bank syariah harus melaporkannya kepada pihak berwenang dan bekerja sama dengan mereka dalam penyelidikan dan penuntutan pelaku kejahatan.

Dalam menghadapi kejahatan siber, upaya pencegahan lebih baik daripada pemulihan. Oleh karena itu, bank syariah harus secara proaktif mengidentifikasi dan mengurangi risiko kejahatan siber melalui penggunaan teknologi keamanan yang canggih, kebijakan dan prosedur yang ketat, serta pelatihan dan kesadaran keamanan yang terus-menerus ditingkatkan.

b) Serangan Malware dan Ransomware

Serangan malware dan ransomware merupakan dua bentuk kejahatan siber yang seringkali merugikan bank syariah dan nasabahnya. 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.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Pemahaman mendalam tentang serangan ini menjadi penting dalam upaya melindungi sistem perbankan syariah dan data sensitif nasabah. (Madakam, 2015)

Serangan malware dapat terjadi melalui berbagai cara, termasuk melalui email, tautan yang meragukan, atau unduhan dari situs web yang tidak terpercaya. Malware dapat memasuki sistem dan menjalankan berbagai tindakan merusak, seperti mencuri data, menghancurkan file, atau mengendalikan komputer secara jarak jauh. Jenis malware yang umum meliputi virus, worm, Trojan horse, dan spyware. Serangan malware dapat menyebabkan kerugian finansial yang signifikan bagi bank syariah, kehilangan data nasabah, dan merusak reputasi bank.

Ransomware adalah jenis serangan malware yang telah menjadi ancaman yang semakin meningkat dalam beberapa tahun terakhir. Ransomware bekerja dengan cara mengenkripsi data pada sistem korban dan kemudian meminta pembayaran tebusan dalam bentuk mata uang kripto untuk mengembalikan akses ke data tersebut. Ransomware biasanya menyebar melalui email yang mengandung lampiran berbahaya atau melalui eksploitasi kerentanan dalam sistem perangkat lunak. Ketika ransomware berhasil mengenkripsi data, nasabah atau bank harus membayar tebusan untuk mendapatkan kunci dekripsi. Serangan ransomware dapat mengakibatkan kerugian finansial yang besar dan mengganggu operasi bank syariah.

Pencegahan dan deteksi dini menjadi kunci dalam melawan serangan malware dan ransomware. Bank syariah harus mengadopsi kebijakan keamanan yang ketat, seperti penerapan solusi keamanan yang canggih, pembaruan perangkat lunak yang teratur, dan pemantauan jaringan yang ketat. Perlindungan data yang kuat, termasuk enkripsi data, juga sangat penting untuk mencegah pencurian dan penyalahgunaan data oleh serangan malware. Selain itu, pelatihan keamanan bagi karyawan dan kesadaran nasabah tentang ancaman malware dan ransomware dapat membantu dalam mengidentifikasi dan mencegah serangan tersebut.

Apabila terjadi serangan malware atau ransomware, respons cepat dan pemulihan yang efektif juga sangat penting. Bank syariah harus memiliki rencana darurat yang telah teruji untuk mengatasi serangan tersebut, termasuk isolasi sistem yang terinfeksi, pemulihan data dari cadangan yang aman, dan kolaborasi dengan pihak keamanan dan penegak hukum dalam menyelidiki serangan tersebut. Serangan malware dan ransomware terus berkembang dan menjadi ancaman yang serius dalam lingkungan teknologi informasi pada bank syariah. Oleh karena itu, penting bagi bank syariah untuk menjaga langkah-langkah keamanan yang proaktif, meningkatkan kesadaran dan pelatihan keamanan bagi karyawan dan nasabah, serta melibatkan lembaga keamanan dan penegak hukum dalam upaya pencegahan, deteksi, dan penanggulangan serangan ini.

c) Phising dan Social Engineering

Phishing dan social engineering merupakan dua metode yang umum digunakan oleh penjahat siber untuk melakukan serangan terhadap bank syariah dan nasabahnya. Kedua metode ini melibatkan manipulasi dan penipuan terhadap manusia dengan tujuan memperoleh informasi sensitif, seperti kata sandi, data keuangan, atau akses ke sistem komputer. Pemahaman yang mendalam tentang phishing dan social engineering menjadi penting dalam upaya melindungi sistem perbankan syariah dan menjaga keamanan data nasabah.

Phishing adalah tindakan meminta (memancing) pengguna komputer untuk mengungkapkan informasi rahasia dengan cara mengirimkan pesan penting palsu, dapat berupa email, website, atau komunikasi elektronik lainnya. (Nurhayani, 2022)

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Phishing adalah metode penipuan online yang umum digunakan dalam serangan kejahatan siber. Dalam serangan phishing, penyerang mengirimkan email atau pesan palsu yang meniru entitas yang tepercaya, seperti bank syariah, dengan tujuan memperoleh informasi sensitif dari nasabah. Email atau pesan tersebut seringkali mengandung tautan yang mengarah ke situs web palsu yang dirancang sedemikian rupa sehingga mirip dengan situs web asli. Jika nasabah mengikuti tautan dan memasukkan informasi sensitif seperti nama pengguna dan kata sandi, penyerang akan memperoleh akses ke akun nasabah tersebut. Serangan phishing juga dapat dilakukan melalui panggilan telepon palsu atau pesan teks yang mengecoh nasabah untuk memberikan informasi pribadi mereka. (A, 2020)

Social engineering adalah metode manipulasi psikologis yang digunakan oleh penjahat siber untuk memanipulasi manusia dan mendapatkan akses ke sistem atau informasi yang sensitif. Penyerang menggunakan teknik manipulasi, seperti memanfaatkan kepercayaan, memancing emosi, atau memanfaatkan kurangnya kesadaran keamanan, untuk memperoleh informasi yang mereka butuhkan. Contoh dari serangan social engineering termasuk penipuan telepon, di mana penyerang berpura-pura menjadi petugas bank dan meminta informasi pribadi dari nasabah, atau serangan penggantian identitas, di mana penyerang mencoba mengaku sebagai karyawan bank untuk mendapatkan akses ke sistem internal.

Untuk melawan phishing dan social engineering, bank syariah perlu mengadopsi pendekatan multilapis dalam keamanan. Hal ini meliputi penerapan filter spam dan email yang kuat untuk mendeteksi dan mencegah email phishing masuk ke kotak masuk nasabah. Edukasi nasabah juga menjadi penting, di mana bank syariah harus memberikan informasi yang jelas tentang tanda-tanda serangan phishing dan bagaimana melindungi diri dari serangan tersebut. Selain itu, pelatihan keamanan bagi karyawan juga penting agar mereka dapat mengenali taktik social engineering dan melindungi informasi sensitif perusahaan. Kerjasama dengan lembaga keamanan siber dan penegak hukum juga penting dalam melawan phishing dan social engineering. Bank syariah dapat bekerja sama dengan lembaga keamanan untuk memperoleh informasi tentang serangan terbaru dan strategi perlindungan yang efektif. Selain itu, jika terjadi serangan phishing atau social engineering, bank syariah harus melaporkan kejadian tersebut kepada pihak berwenang dan bekerja sama dalam penyelidikan dan penegakan hukum terhadap pelaku kejahatan.

Selain itu, Penerapan teknologi keamanan juga merupakan langkah penting dalam melawan phishing dan social engineering. Bank syariah perlu mengadopsi solusi keamanan yang canggih, seperti firewall, sistem deteksi intrusi, dan keamanan jaringan yang kuat untuk melindungi sistem mereka dari serangan yang berpotensi. Selain itu, penggunaan teknologi autentikasi yang kuat, seperti verifikasi dua faktor, dapat memberikan lapisan keamanan tambahan untuk melindungi akun nasabah dari serangan phishing. (Ghasemi, 2018)

d) Pelanggaran Data dan Pencurian Identitas

Pelanggaran data dan pencurian identitas merupakan ancaman serius dalam lingkungan teknologi informasi pada bank syariah. Pelanggaran data terjadi ketika informasi sensitif, seperti data pribadi nasabah atau informasi keuangan, diretas, diakses, atau diperoleh oleh pihak yang tidak berwenang. Pencurian identitas, di sisi lain, terjadi ketika data pribadi seseorang digunakan oleh penjahat siber untuk mengakses akun atau melakukan kegiatan ilegal atas nama korban. Pemahaman yang

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

mendalam tentang pelanggaran data dan pencurian identitas menjadi penting dalam melindungi keamanan dan privasi nasabah bank syariah.

Pelanggaran data dapat terjadi melalui berbagai cara, termasuk serangan siber, kebocoran data, atau penyalahgunaan oleh pihak internal. Penyerang dapat memanfaatkan kerentanan dalam sistem perbankan untuk mendapatkan akses ke data sensitif nasabah atau menggunakan teknik seperti serangan phishing atau malware untuk mencuri informasi. Kebocoran data juga dapat terjadi melalui kesalahan manusia, seperti kehilangan perangkat atau ketidakhati-hatian dalam mengelola data sensitif. Pelanggaran data dapat memiliki konsekuensi yang serius, termasuk kerugian finansial bagi bank syariah dan nasabah, kerusakan reputasi, dan potensi pelanggaran privasi.

Pencurian identitas melibatkan penggunaan data pribadi seseorang, seperti nama, tanggal lahir, atau nomor kartu identitas, untuk tujuan penipuan atau akses ilegal. Penjahat siber dapat menggunakan data tersebut untuk membuka akun palsu, melakukan transaksi keuangan ilegal, atau bahkan melakukan kegiatan kriminal dengan identitas korban. Pencurian identitas seringkali terjadi melalui serangan phishing, di mana penyerang memperoleh informasi sensitif dari nasabah yang tidak curiga melalui email palsu atau situs web palsu. Selain itu, pencurian identitas juga dapat terjadi melalui serangan malware atau kebocoran data di dalam bank syariah.

Untuk melawan pelanggaran data dan pencurian identitas, bank syariah perlu mengadopsi langkah-langkah keamanan yang kuat. Perlindungan data yang kuat, seperti enkripsi dan pengamanan akses, harus diterapkan untuk mencegah akses yang tidak sah ke data sensitif nasabah. Pelatihan keamanan bagi karyawan juga penting agar mereka dapat mengenali tanda-tanda serangan dan melindungi data secara efektif. Selain itu, bank syariah harus melibatkan tim keamanan yang terlatih dan bekerja sama dengan lembaga keamanan siber untuk memantau dan mendeteksi ancaman keamanan yang potensial.

Penegakan hukum juga menjadi aspek penting dalam melawan pelanggaran data dan pencurian identitas. Bank syariah harus melaporkan pelanggaran ke pihak berwenang dan bekerja sama dalam penyelidikan dan penegakan hukum terhadap pelaku kejahatan. Selain itu, bank syariah juga harus memberikan perlindungan yang memadai kepada nasabah yang menjadi korban pelanggaran data atau pencurian identitas. Hal ini termasuk memberikan bantuan dalam memulihkan akun dan mengamankan informasi pribadi nasabah yang terkena dampak.

Pada tingkat teknis, bank syariah harus mengadopsi kebijakan keamanan yang ketat, termasuk penggunaan firewall yang kuat, pemantauan jaringan yang terus-menerus, serta pembaruan dan pemeliharaan sistem yang teratur. Selain itu, penting untuk melakukan audit keamanan secara berkala guna mengidentifikasi dan mengatasi kerentanan potensial dalam sistem.

Beberapa langkah lain yang dapat diambil untuk melindungi nasabah dari pelanggaran data dan pencurian identitas adalah dengan menerapkan proses verifikasi yang ketat saat membuka akun, seperti verifikasi dua faktor. Selain itu, bank syariah juga dapat mengedukasi nasabah mengenai praktik keamanan yang baik, seperti pentingnya menggunakan kata sandi yang kuat, tidak membagikan informasi pribadi secara sembarangan, dan melaporkan kejadian yang mencurigakan segera kepada pihak bank.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

3.2. Tantangan dalam Menghadapi Ancaman Terkini

Dalam menghadapi ancaman terkini terkait risiko teknologi informasi pada bank syariah, terdapat beberapa tantangan yang perlu diatasi agar keamanan sistem perbankan tetap terjaga. Berdasarkan pembahasan sebelumnya, beberapa tantangan tersebut meliputi evolusi serangan, kompleksitas teknologi, kurangnya kesadaran keamanan, dan kurangnya sumber daya yang memadai.Pertama, evolusi serangan menjadi tantangan utama dalam menghadapi ancaman terkini. Penjahat siber terus mengembangkan metode dan teknik mereka, sehingga memerlukan respons yang cepat dan adaptif dari bank syariah. Ancaman seperti serangan phishing, social engineering, malware, dan ransomware terus berkembang dan semakin canggih. Penyerang menggunakan teknik baru, memanfaatkan kerentanan yang belum terdeteksi, dan mencari celah dalam sistem keamanan yang ada. Oleh karena itu, bank syariah perlu tetap memantau perkembangan tren kejahatan siber, berkolaborasi dengan lembaga keamanan siber, dan mengadopsi solusi keamanan yang terkini. (RI, 2019)

Kedua, kompleksitas teknologi menjadi tantangan lain yang dihadapi dalam menjaga keamanan bank syariah. Dalam lingkungan perbankan yang modern, terdapat berbagai macam sistem, aplikasi, perangkat, dan jaringan yang saling terhubung. Keberagaman teknologi ini menciptakan lanskap yang rumit dan meningkatkan potensi kerentanan. Selain itu, perkembangan teknologi seperti Internet of Things (IoT) dan komputasi awan juga memperluas permukaan serangan. Bank syariah harus mampu mengelola dan mengamankan infrastruktur teknologi mereka dengan baik, termasuk melindungi data di dalam dan di luar jaringan, serta mengadopsi kebijakan keamanan yang memadai.

Ketiga, kurangnya kesadaran keamanan menjadi tantangan yang perlu diatasi. Meskipun bank syariah menerapkan berbagai langkah keamanan, nasabah dan karyawan yang kurang sadar akan praktik keamanan berisiko tinggi dapat menjadi celah bagi serangan. Nasabah yang tidak menyadari tanda-tanda serangan phishing atau kurang berhati-hati dalam membagikan informasi pribadi dapat menjadi sasaran empuk bagi penyerang. Selain itu, kurangnya kesadaran keamanan di kalangan karyawan dapat menyebabkan kesalahan manusia yang dapat dieksploitasi oleh penjahat siber. Oleh karena itu, edukasi dan pelatihan keamanan yang terus-menerus kepada nasabah dan karyawan bank syariah menjadi penting untuk meningkatkan kesadaran akan ancaman keamanan dan cara melindungi diri.

Keempat, kurangnya sumber daya yang memadai dapat menjadi tantangan dalam menghadapi ancaman terkini. Perlindungan keamanan yang efektif membutuhkan investasi yang signifikan dalam infrastruktur teknologi, solusi keamanan, dan sumber daya manusia yang terlatih di bidang keamanan siber. Namun, banyak bank syariah, terutama yang berukuran kecil, mungkin mengalami keterbatasan sumber daya, baik dari segi keuangan maupun keahlian. Hal ini dapat mempengaruhi kemampuan mereka untuk mengadopsi teknologi keamanan yang canggih, mempekerjakan tenaga ahli keamanan yang berkualitas, atau melaksanakan pelatihan keamanan yang intensif. Oleh karena itu, bank syariah perlu mencari solusi yang memadai, seperti melibatkan mitra keamanan ciber eksternal, berkolaborasi dengan lembaga keamanan siber, atau menggunakan layanan keamanan berbasis cloud yang dapat memberikan keamanan tambahan tanpa membebani sumber daya internal yang terbatas.

Selain itu, tantangan dalam menghadapi ancaman terkini juga meliputi kepatuhan terhadap regulasi dan kebijakan privasi yang semakin ketat. Bank syariah harus mematuhi peraturan dan standar keamanan yang ditetapkan oleh regulator, seperti peraturan perlindungan data pribadi dan peraturan keamanan informasi. Hal ini melibatkan

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

pemantauan dan pemenuhan persyaratan kepatuhan yang terus berubah, yang dapat membutuhkan upaya tambahan dan sumber daya yang signifikan.

3.3 Implementasi Sistem Keamanan Yang Tepat

Dalam menghadapi ancaman terkini terkait risiko teknologi informasi pada bank syariah, implementasi sistem keamanan yang tepat menjadi kunci untuk melindungi sistem perbankan dan informasi nasabah. Berdasarkan pembahasan sebelumnya, beberapa langkah dapat diambil dalam mengimplementasikan sistem keamanan yang efektif, termasuk identifikasi dan evaluasi risiko, penggunaan teknologi keamanan yang mutakhir, pengawasan dan pemantauan yang aktif, serta pelatihan dan kesadaran keamanan yang terus-menerus.

Pertama, langkah awal dalam implementasi sistem keamanan yang tepat adalah identifikasi dan evaluasi risiko. Bank syariah perlu melakukan analisis risiko secara menyeluruh untuk mengidentifikasi ancaman dan kerentanan potensial dalam sistem mereka. Hal ini melibatkan pemahaman mendalam tentang lingkungan perbankan, aplikasi, jaringan, dan infrastruktur yang digunakan, serta ancaman terkini yang mungkin terjadi. Dengan melakukan identifikasi risiko yang komprehensif, bank syariah dapat mengembangkan strategi keamanan yang tepat dan menetapkan prioritas dalam melindungi aset penting.

Kedua, penggunaan teknologi keamanan yang mutakhir menjadi langkah penting dalam menghadapi ancaman terkini. Bank syariah perlu mengadopsi solusi keamanan yang canggih untuk melindungi sistem mereka dari serangan. Ini termasuk penggunaan firewall yang kuat, sistem deteksi intrusi, enkripsi data, serta solusi anti-malware dan anti-phishing yang efektif. Selain itu, teknologi keamanan seperti autentikasi dua faktor, kontrol akses yang ketat, dan pemantauan jaringan yang terus-menerus juga dapat membantu dalam mengurangi risiko keamanan.

Ketiga, pengawasan dan pemantauan yang aktif merupakan langkah penting dalam mengimplementasikan sistem keamanan yang tepat. Bank syariah perlu memiliki mekanisme pemantauan yang terus-menerus untuk mendeteksi serangan atau perilaku yang mencurigakan dalam jaringan mereka. Ini dapat melibatkan penggunaan sistem log dan audit yang memadai, analisis kejadian keamanan secara real-time, serta pemantauan aktivitas pengguna dan lalu lintas jaringan. Dengan memiliki pemantauan yang aktif, bank syariah dapat menangkap dan menanggapi serangan dengan cepat, mengurangi dampak yang mungkin terjadi.

Keempat, pelatihan dan kesadaran keamanan yang terus-menerus merupakan langkah penting dalam melibatkan semua pihak terkait dalam menjaga keamanan sistem. Bank syariah perlu mengadakan pelatihan keamanan reguler untuk karyawan mereka, termasuk pemahaman tentang serangan yang terkini, praktik keamanan yang baik, dan tindakan yang harus diambil dalam menghadapi insiden keamanan. Selain itu, nasabah juga perlu diberikan edukasi mengenai ancaman keamanan yang mungkin mereka hadapi, praktik keamanan dalam penggunaan perangkat perbankan online, dan tanda-tanda serangan yang perlu diwaspadai. Dengan meningkatkan kesadaran keamanan, bank syariah dapat melibatkan semua pihak terkait dalam menjaga keamanan sistem dan melindungi informasi penting.

Selain langkah-langkah di atas, bank syariah juga perlu memperhatikan faktor-faktor penting lainnya dalam implementasi sistem keamanan yang tepat. Pertama, kebijakan dan prosedur keamanan yang jelas dan terdokumentasi harus diimplementasikan. Bank syariah perlu memiliki kebijakan keamanan yang mengatur penggunaan dan akses terhadap sistem,

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

perlindungan data nasabah, tindakan respons terhadap insiden keamanan, dan kepatuhan terhadap regulasi yang berlaku. Kebijakan ini harus diterapkan secara konsisten dan dipahami oleh semua pihak terkait.

Kedua, penting untuk melakukan evaluasi dan pengujian keamanan secara teratur. Bank syariah harus menjalankan pengujian keamanan seperti penetrasi tes dan simulasi serangan untuk menguji ketahanan sistem mereka terhadap serangan nyata. Melalui pengujian ini, kerentanan dan kelemahan sistem dapat diidentifikasi dan diperbaiki sebelum serangan sebenarnya terjadi.

Ketiga, penting untuk menjaga kepatuhan terhadap regulasi dan kebijakan privasi yang berlaku. Bank syariah harus memahami dan mematuhi persyaratan kepatuhan yang ditetapkan oleh otoritas pengawas dan peraturan privasi, seperti perlindungan data pribadi dan keamanan informasi. Mengimplementasikan kontrol keamanan dan praktik kepatuhan yang tepat adalah kunci untuk menjaga reputasi bank syariah dan memenuhi harapan nasabah terkait privasi dan keamanan.

Implementasi sistem keamanan yang tepat merupakan langkah krusial dalam melindungi bank syariah dari ancaman terkini dalam teknologi informasi. Dengan mengidentifikasi dan mengelola risiko, menggunakan teknologi keamanan yang mutakhir, melakukan pengawasan dan pemantauan yang aktif, serta meningkatkan pelatihan dan kesadaran keamanan, bank syariah dapat mengurangi risiko serangan dan melindungi sistem mereka dengan lebih efektif. (Richard, 2010)

4. Simpulan

Ancaman terkini terkait risiko teknologi informasi pada bank syariah merupakan tantangan yang signifikan dalam menjaga keamanan sistem perbankan dan melindungi informasi nasabah. Dalam menghadapi tantangan ini, beberapa langkah penting dapat diambil dalam implementasi sistem keamanan yang tepat.Pertama, identifikasi dan evaluasi risiko merupakan langkah awal yang penting. Dengan melakukan analisis risiko yang komprehensif, bank syariah dapat mengidentifikasi ancaman potensial dan kerentanan dalam sistem mereka. Ini memungkinkan pengembangan strategi keamanan yang tepat dan penentuan prioritas dalam melindungi aset penting.

Kedua, penggunaan teknologi keamanan yang mutakhir sangat penting dalam melawan ancaman terkini. Solusi keamanan seperti firewall yang kuat, sistem deteksi intrusi, enkripsi data, dan solusi anti-malware dan anti-phishing yang efektif dapat membantu melindungi sistem perbankan dari serangan. Selain itu, teknologi keamanan seperti autentikasi dua faktor, kontrol akses yang ketat, dan pemantauan jaringan yang terus-menerus juga penting dalam mengurangi risiko keamanan.

Ketiga, pengawasan dan pemantauan yang aktif adalah langkah penting dalam melindungi sistem. Bank syariah perlu memiliki mekanisme pemantauan yang terus-menerus untuk mendeteksi serangan atau perilaku yang mencurigakan dalam jaringan mereka. Pemantauan yang aktif memungkinkan bank untuk menangkap dan menanggapi serangan dengan cepat, mengurangi dampak yang mungkin terjadi.

Keempat, pelatihan dan kesadaran keamanan yang terus-menerus sangat penting. Bank syariah perlu memberikan pelatihan keamanan reguler kepada karyawan dan juga edukasi kepada nasabah. Dengan meningkatkan kesadaran keamanan, bank dapat melibatkan semua pihak terkait dalam menjaga keamanan sistem dan melindungi informasi penting.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Implementasi sistem keamanan yang tepat membutuhkan pendekatan yang holistik dan terintegrasi. Bank syariah harus mengadopsi kebijakan dan prosedur keamanan yang jelas dan terdokumentasi, melakukan evaluasi dan pengujian keamanan secara teratur, serta mematuhi regulasi dan kebijakan privasi yang berlaku.

Meskipun langkah-langkah tersebut dapat membantu dalam melawan ancaman terkini, penting untuk menyadari bahwa keamanan tidak pernah menjadi upaya yang statis. Ancaman keamanan terus berkembang, dan bank syariah harus terus meningkatkan dan mengadaptasi sistem keamanan mereka sesuai dengan perkembangan tersebut. Kolaborasi dengan lembaga keamanan siber, partisipasi dalam komunitas keamanan, dan pembaruan teknologi keamanan yang terus-menerus adalah faktor penting dalam menghadapi ancaman terkini.

Dalam kesimpulan, menghadapi ancaman terkini terkait risiko teknologi informasi pada bank syariah memerlukan implementasi sistem keamanan yang tepat. Dengan identifikasi dan evaluasi risiko yang komprehensif, penggunaan teknologi keamanan yang mutakhir, pengawasan dan pemantauan yang aktif, serta pelatihan dan kesadaran keamanan yang terus-menerus, bank syariah dapat mengurangi risiko serangan dan melindungi sistem perbankan mereka dengan lebih efektif. Implementasi kebijakan keamanan yang jelas, evaluasi dan pengujian keamanan teratur, serta pematuhan terhadap regulasi dan kebijakan privasi juga merupakan faktor penting dalam menjaga keamanan sistem.

Namun, penting untuk diingat bahwa implementasi sistem keamanan yang tepat bukanlah upaya satu kali. Ancaman keamanan terus berkembang, dan bank syariah harus tetap waspada terhadap ancaman baru yang muncul. Kolaborasi dengan lembaga keamanan siber dan partisipasi dalam komunitas keamanan dapat memberikan informasi terkini tentang tren dan serangan yang baru muncul, sehingga bank dapat mengambil tindakan yang sesuai.

5. Ucapan Terimakasih

Penulis ingin mengucapkan terima kasih kepada para pembaca atas perhatian dan waktu yang telah diberikan untuk membaca artikel ini. Pembahasan mengenai analisis risiko teknologi informasi pada bank syariah dan identifikasi tantangan terkini merupakan topik yang kompleks dan krusial dalam dunia perbankan digital saat ini. Dalam proses penulisan artikel ini, penulis telah belajar banyak tentang ancaman terkini yang dihadapi oleh bank syariah dalam menjaga keamanan sistem mereka. Melalui penelitian dan studi literatur yang mendalam, penulis berharap artikel ini dapat memberikan pemahaman yang lebih baik tentang risiko teknologi informasi dan langkah-langkah yang dapat diambil untuk menghadapinya.

Penulis juga ingin mengucapkan terima kasih kepada para peneliti, ahli keamanan, dan pengamat industri yang telah berkontribusi dalam menghasilkan pengetahuan dan informasi yang menjadi dasar artikel ini. Referensi yang digunakan dalam artikel ini telah memberikan pemahaman yang mendalam tentang isu-isu keamanan teknologi informasi dalam konteks perbankan syariah. Selain itu, penulis ingin mengapresiasi upaya bank syariah dan institusi keuangan lainnya dalam menjaga keamanan sistem dan melindungi nasabah dari serangan siber. Dalam dunia yang semakin kompleks dan terhubung secara digital, tindakan proaktif dan implementasi sistem keamanan yang tepat sangat penting untuk menjaga kepercayaan nasabah dan melindungi informasi pribadi.Terakhir, penulis

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

berharap bahwa artikel ini dapat memberikan sumbangsih yang bermanfaat dalam memahami dan mengatasi tantangan keamanan teknologi informasi yang dihadapi oleh bank syariah. Kesadaran dan pemahaman yang meningkat tentang risiko dan ancaman terkini dapat membantu bank syariah dalam mengambil langkah-langkah yang efektif untuk melindungi sistem dan data nasabah.

Sekali lagi, penulis mengucapkan terima kasih atas kesempatan ini dan berharap artikel ini memberikan wawasan yang berharga dalam menjaga keamanan teknologi informasi pada bank syariah. Semoga artikel ini dapat menjadi panduan yang bermanfaat bagi pembaca dalam memahami dan menghadapi ancaman terkini yang berkembang pesat di dunia digital. Terima kasih.

Daftar Pustaka

A Survey on Phishing And It's Detection Techniques Based on Support Vector Method (SVM) and Software Defined Networking(SDN) (2020.)

Ariffin, N. M., & Kassim, S. (2014). Risk Management Practices Of Selected Islamic Banks In Malaysia. Aceh *International Journal Of Social Science*s, 3(1), 26–36.

Bruce C. (2015). Data and Goliath.

Corne, T. C. (2020). Legal Protection Of Privacy Data Through Encryption Technology. Lampung *Journal of International Law,* 1(2), 63–70. Https://doi.org/10.25041/lajil.v1i2.2027.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Papers on Risk and Insurance*: Issues and Practice, 47(3), 698–736. Https://doi.org/10.1057/s41288-022-00266-6.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law and Security Review, 34(2), 193–203. Https://doi.org/10.1016/j.clsr.2017.10.003.

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.

Jakobsson, M., & Myers, S. (2020.). Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft. Www.swsec.

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. In The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. *Springer Berlin Heidelberg*. Https://doi.org/10.1007/978-3-642-11522-6.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 03(05), 164–173. Https://doi.org/10.4236/jcc.2015.35021.

Mohaghar, A., Reza, M., Moghadam, S., Beigi, R. G., & Ghasemi, R. (2018.). IoT-Based Services in Banking Industry Using a Business Continuity Management Approach. Https://doi.org/10.22059/JITM.2021.314908.2666.

Asy-Syarikah
Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam
Volume 5, No. 2, 2023
ISSN (print) : 2656-6117
ISSN (online) : 2715-0356
Homepage : http://journal.uiad.ac.id/index.php/asy-syarikah

Nurwahida, N., Dianita, I., & Nurhayani, N. (2022). Proses Transaksi Pada Sistem Informasi Akuntansi Serta Implementasinya Pada Perbankan Syariah. *Jurnal Asy-Syarikah*: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam, 4(1), 81-91. \

Pertahanan Siber, P. (2019.). Kementerian Pertahanan RI.

Somayaji, Anil., Ford, Richard., Association for Computing Machinery., & ACM Digital Library. (2010). Proceedings of the 2009 workshop on New Security Paradigms Workshop. Association for Computing Machinery.