MUSYTARI
ISSN : 3025-9495

Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

CYBER RISK MANAGEMENT DALAM INDUSTRI PERBANKAN DIGITAL

Muhammad Abdul Hafizh[1], Arsyadona[2],Ade Aulia Riski[3], Tyo nugro diningrat[4], al balkhi yahya sinuraya[5] abdlhafizh16@gmail.com[1], arsyadona1100000174@uinsu.ac.id[2], Adeaulia71213@gmail.com[3], tyodiningrat17@gmail.com[4], albalkhiyahya@gmail.com[5]
Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara Medan

Abstrak

Dalam era digital yang semakin maju, industri perbankan digital menghadapi berbagai ancaman siber yang dapat merugikan baik institusi maupun nasabahnya. Manajemen risiko siber menjadi sangat penting untuk melindungi informasi sensitif dan mempertahankan kepercayaan pelanggan. Artikel ini membahas pentingnya manajemen risiko siber di perbankan digital, termasuk jenis-jenis ancaman siber yang umum, seperti phishing, ransomware, dan serangan distributed denial-of-service (DdoS). Selain itu, artikel ini mengidentifikasi kerentanan yang sering terjadi dalam sistem perbankan digital dan strategi efektif untuk mitigasi risiko, seperti penerapan enkripsi, autentikasi multi-faktor, serta penilaian keamanan berkala. Studi kasus terkait serangan siber di sektor perbankan menunjukkan pentingnya langkah proaktif dalam menjaga keamanan data. Artikel ini juga menyoroti pentingnya kepatuhan terhadap regulasi yang berlaku untuk memastikan keamanan yang optimal dalam menghadapi ancaman yang terus berkembang. Dengan strategi manajemen risiko siber yang kuat, bank digital dapat melindungi data sensitif, menjaga reputasi, dan memperkuat posisi keamanan mereka.

Kata Kunci : Manajemen Risiko Siber, Perbankan Digital, Keamanan Siber, Ancaman Siber, Enkripsi, Regulasi Keamanan.

Received: Januari 2025
Reviewed: Januari 2025
Published: Januari 2025

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/Musytari.v1i2.365
Copyright : Author
Publish by : Musytari

Pendahuluan

Definisi manajemen risiko siber

Manajemen resiko siber adalah proses mengidentifikasi, menilai dan memitigasi potensi risiko terhadap sistem dan data teknologi informasi suatu organisasi (Alice & Alexis, 2002). Ini melibatkan penerapan strategi dan kontrol untuk melindungi terhadap ancaman siber, seperti peretasan, malware, dan pelanggaran data. Manajemen risiko siber yang efektif sangat penting untuk melindungi informasi sensitif dan menjaga kepercayaan pelanggan serta pemangku kepentingan. Dengan secara proaktif mengelola risiko siber, organisasi dapat mengurangi kemungkinan dan dampak serangan siber, yang pada akhirnya melindungi reputasi dan stabilitas keuangan mereka. Melakukan audit keamanan secara rutin dan tetap memperbarui informasi tentang ancaman siber terbaru adalah komponen penting dalam manajemen risiko siber. Selain itu, membuat rencana tanggapan untuk potensi insiden keamanan dapat membantu meminimalkan kerusakan dan memastikan pemulihan yang cepat.

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Dengan berinvestasi dalam langkah-langkah keamanan siber dan terus memantau serta meningkatkan protokol keamanan, organisasi dapat lebih baik mempertahankan diri terhadap ancaman siber yang berkembang dan menjaga pertahanan yang kuat terhadap potensi serangan. Pada akhirnya, memprioritaskan manajemen resiko siber sangat penting untuk memeastikan keberhasilan jangka Panjang dan ketahanan suatu organisasi di lanskap digital saat ini. Misalnya, sebuah Perusahaan dapat melakukan penilaian kerentanan secara berkala dan pengujian penetrasi untuk mengidentifikasi dan mengatasi potensi kelemahan dalam system mereka. Dalam hal terjadinya pelanggaran keamanan, memiliki tim respons insiden dengan protocol yang jelas untuk menangani dan mengurangi serangan dapat membantu meminimalkan waktu henti dan kehilangan data.

Pentingnya manajemen risiko siber dalam industri perbankan digital

Dalam industri perbankan digital, pentingnya manajemen risiko siber tidak dapat diremehkan. With the increasing reliance on technology for financial transactions and customer data storage, banks are prime targets for cyber criminals looking to exploit vulnerabilities in their systems (Samuel et al., 2023) . Pelanggaran keamanan tidak hanya dapat mengakibatkan kerugian finansial bagi bank, tetapi juga mengikis kepercayaan pelanggan dan merusak reputasi mereka. Oleh karena itu, bank harus berinvestasi dalam langkah-langkah keamanan siber yang kuat untuk melindungi aset mereka dan menjaga integritas layanan mereka. Ini termasuk menerapkan protokol keamanan berlapis, teknik enkripsi, dan pemantauan terus-menerus terhadap aktivitas jaringan untuk mendeteksi dan merespons potensi ancaman secara real-time. Dengan tetap proaktif dan waspada dalam pendekatan mereka terhadap manajemen risiko siber, bank dapat melindungi diri dari potensi serangan dan memastikan keselamatan serta keamanan operasi mereka. Misalnya, sebuah bank yang gagal mengamankan platform perbankan online mereka dengan baik bisa menjadi korban serangan siber di mana informasi sensitif pelanggan dicuri. Ini dapat mengakibatkan kerugian finansial yang signifikan bagi bank dan pelanggannya, serta merusak reputasi bank. Untuk mencegah hal ini, bank dapat berinvestasi dalam langkah-langkah keamanan siber yang canggih seperti otentikasi biometrik, enkripsi data, dan audit keamanan reguler untuk melindungi dari potensi ancaman. Namun, meskipun dengan langkah-langkah ini diterapkan, seorang peretas yang canggih masih bisa menemukan cara untuk membobol sistem. Pada tahun 2014, JPMorgan Chase mengalami serangan siber besar-besaran yang mengkompromikan informasi pribadi dari 76 juta rumah tangga dan 7 juta usaha kecil, meskipun telah memiliki protokol keamanan yang kuat.(Thomas & Phil, 2016). Oleh karena itu, sangat penting bagi bank untuk terus memperbarui diri dengan tren dan teknologi keamanan siber terbaru agar tetap unggul dari para peretas. Melatih karyawan secara rutin tentang cara mengenali dan merespons potensi ancaman siber juga penting dalam menjaga pertahanan yang kuat. Selain itu, menetapkan rencana respons cepat dalam hal terjadinya pelanggaran dapat membantu meminimalkan kerusakan dan meningkatkan peluang untuk mengidentifikasi serta menangkap para peretas. Dengan mengambil langkah-langkah proaktif ini, bank dapat lebih baik melindungi diri mereka sendiri dan pelanggan mereka dari konsekuensi menghancurkan dari serangan siber.

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Ancaman Siber dalam Industri Perbankan Digital

Jenis-jenis ancaman siber yang dihadapi oleh bank digital

Termasuk serangan phishing, ransomware, malware, dan serangan distributed denial-of-service (DDoS). Serangan phishing melibatkan upaya penipuan untuk memperoleh informasi sensitif seperti kredensial login atau data keuangan melalui email atau situs web yang menipu. Ransomware adalah jenis malware yang mengenkripsi file pengguna dan menuntut pembayaran untuk pembebasannya. Malware, di sisi lain, adalah perangkat lunak berbahaya yang dirancang untuk mengganggu atau merusak sistem komputer. Serangan DDoS melibatkan membanjiri jaringan atau server dengan arus lalu lintas yang besar, membuatnya tidak dapat diakses oleh pengguna yang sah. Ancaman siber ini menimbulkan risiko signifikan bagi bank digital dan pelanggan mereka, menyoroti pentingnya langkah- langkah keamanan yang kuat dan strategi pertahanan proaktif. Menerapkan otentikasi multi-

faktor, pembaruan keamanan secara berkala, dan pelatihan karyawan untuk mengenali upaya phishing adalah langkah-langkah penting bagi bank digital untuk melindungi diri dari ancaman siber ini. Selain itu, berinvestasi dalam teknologi deteksi ancaman canggih dan menjalin kemitraan dengan ahli keamanan siber dapat membantu mengurangi risiko serangan ransomware, malware, dan DDoS. Dengan tetap waspada dan proaktif dalam praktik keamanan mereka, bank digital dapat melindungi sistem dan data pelanggan mereka dari potensi pelanggaran dan kerugian finansial.

Kerentanan umum dalam sistem perbankan digital

Termasuk kata sandi yang lemah, transmisi data yang tidak terenkripsi, dan kurangnya autentikasi multi-faktor. Kerentanan ini dapat dieksploitasi oleh penjahat siber untuk mendapatkan akses tidak sah ke informasi sensitif, memanipulasi transaksi, dan mengganggu layanan. Sangat penting bagi bank digital untuk melakukan penilaian keamanan secara berkala dan pengujian penetrasi guna mengidentifikasi dan mengatasi setiap kelemahan dalam sistem mereka. Menerapkan langkah-langkah keamanan yang kuat, seperti enkripsi, firewall, dan sistem deteksi intrusi, dapat membantu mencegah akses tidak sah dan melindungi data pelanggan dari ancaman siber. Selain itu, memastikan kepatuhan terhadap regulasi dan standar industri, seperti PCI DSS dan GDPR, dapat membantu bank digital menjaga lingkungan yang aman dan terpercaya bagi pelanggan mereka. Dengan tetap waspada dan proaktif dalam pendekatan mereka terhadap keamanan siber, bank digital dapat tetap selangkah lebih maju dari penjahat siber dan melindungi informasi sensitif pelanggan mereka. Dalam lanskap ancaman keamanan siber yang terus berkembang, penting bagi bank digital untuk terus memperbarui dan meningkatkan protokol keamanan mereka agar dapat beradaptasi dengan tantangan baru. Pada akhirnya, memprioritaskan keamanan siber sangat penting bagi bank digital untuk membangun dan mempertahankan kepercayaan dengan pelanggan mereka serta memastikan keberhasilan jangka panjang bisnis mereka.

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Kerentanan umum dalam sistem perbankan digital

Termasuk kata sandi yang lemah, transmisi data yang tidak terenkripsi, dan kurangnya autentikasi multi-faktor. Kerentanan ini dapat dieksploitasi oleh penjahat siber untuk mendapatkan akses tidak sah ke informasi sensitif, memanipulasi transaksi, dan mengganggu layanan. Sangat penting bagi bank digital untuk melakukan penilaian keamanan secara berkala dan pengujian penetrasi guna mengidentifikasi dan mengatasi setiap kelemahan dalam sistem mereka. Menerapkan langkah-langkah keamanan yang kuat, seperti enkripsi, firewall, dan sistem deteksi intrusi, dapat membantu mencegah akses tidak sah dan melindungi data pelanggan dari ancaman siber. Selain itu, memastikan kepatuhan terhadap regulasi dan standar industri, seperti PCI DSS dan GDPR, dapat membantu bank digital menjaga lingkungan yang aman dan terpercaya bagi pelanggan mereka. Dengan tetap waspada dan proaktif dalam pendekatan mereka terhadap keamanan siber, bank digital dapat tetap selangkah lebih maju dari penjahat siber dan melindungi informasi sensitif pelanggan mereka. Dalam lanskap ancaman keamanan siber yang terus berkembang, penting bagi bank digital untuk terus memperbarui dan meningkatkan protokol keamanan mereka agar dapat beradaptasi dengan tantangan baru. Pada akhirnya, memprioritaskan keamanan siber sangat penting bagi bank digital untuk membangun dan mempertahankan kepercayaan dengan pelanggan mereka serta memastikan keberhasilan jangka panjang bisnis mereka.

Studi kasus serangan siber pada bank digital

Menyoroti pentingnya mengambil langkah-langkah proaktif untuk melindungi dari potensi ancaman. Salah satu studi kasus tersebut melibatkan serangan phishing yang canggih yang menargetkan pelanggan dari sebuah bank digital terkemuka, yang mengakibatkan kerugian finansial yang signifikan dan kerusakan reputasi. Insiden ini menekankan perlunya bank digital untuk berinvestasi dalam langkah-langkah keamanan yang kuat, seperti autentikasi multi-faktor dan enkripsi, untuk mencegah akses tidak sah ke data pelanggan yang sensitif. Selain itu, pemantauan berkelanjutan dan berbagi intelijen ancaman dapat membantu bank digital mengidentifikasi dan merespons ancaman siber yang muncul sebelum berkembang menjadi serangan besar. Dengan belajar dari insiden masa lalu dan menerapkan praktik terbaik dalam keamanan siber, bank digital dapat lebih baik melindungi pelanggan mereka dan menjaga reputasi mereka sebagai lembaga keuangan yang tepercaya. Misalnya, pada tahun 2019, sebuah bank digital mengalami pelanggaran data akibat kerentanan dalam sistem otentikasi mereka, yang mengakibatkan akses tidak sah ke akun pelanggan. Akibatnya, bank tersebut mengalami kerusakan reputasi dan kerugian finansial, yang menyoroti pentingnya langkah-langkah keamanan yang kuat dalam industri perbankan digital.

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Meskipun penting bagi bank digital untuk belajar dari insiden masa lalu dan menerapkan praktik terbaik dalam keamanan siber, adalah mustahil untuk sepenuhnya menghilangkan semua ancaman keamanan siber. Tidak ada sistem yang kebal terhadap serangan, dan penjahat siber terus mengembangkan taktik mereka untuk menghindari langkah-langkah keamanan. Oleh karena itu, sangat penting bagi bank digital untuk tetap waspada.nd proactive in detecting and responding to potential threats. Ini termasuk secara teratur memperbarui sistem keamanan mereka, melakukan penilaian risiko yang menyeluruh, dan memberikan pelatihan berkelanjutan bagi karyawan untuk mengenali dan mencegah serangan siber. Dengan tetap unggul dari para penjahat siber dan terus meningkatkan langkah-langkah keamanan mereka, bank digital dapat lebih baik melindungi informasi sensitif pelanggan mereka dan mempertahankan kepercayaan dalam industri perbankan digital.

Strategi Manajemen Risiko Siber

Menerapkan enkripsi dan autentikasi multi-faktor

protokol otentikasi sangat penting dalam melindungi data sensitif dan mencegah akses tidak sah. Selain itu, bank digital harus secara teratur memantau jaringan mereka untuk aktivitas mencurigakan dan memiliki rencana respons insiden untuk segera menangani pelanggaran keamanan. Berkolaborasi dengan ahli keamanan siber dan tetap mendapatkan informasi tentang ancaman dan tren terbaru di industri juga dapat membantu bank digital tetap selangkah lebih maju dari penjahat siber. Dengan memprioritaskan keamanan siber dan menerapkan strategi manajemen risiko yang kuat, bank digital dapat secara efektif melindungi sistem mereka dan menjaga integritas layanan mereka. Misalnya, bank digital dapat menggunakan autentikasi multi-faktor untuk login pelanggan dan mengenkripsi data sensitif untuk melindungi dari ancaman siber. Dalam hal terjadi pelanggaran keamanan, bank dapat mengaktifkan rencana respons insiden mereka untuk mengatasi pelanggaran tersebut, menyelidiki penyebabnya, dan menerapkan langkah-langkah untuk mencegah serangan di masa depan. Meskipun langkah-langkah ini penting untuk mencegah dan merespons ancaman siber, sangat penting bagi bank untuk terus memperbarui dan meningkatkan protokol keamanan mereka agar tetap unggul dalam menghadapi ancaman siber yang terus berkembang. Selain itu, mengandalkan hanya pada langkah-langkah reaktif mungkin tidak cukup dalam lanskap keamanan siber yang cepat berubah saat ini. Langkah-langkah proaktif, seperti melakukan audit keamanan secara berkala, menerapkan otentikasi multi-faktor, dan memberikan pelatihan berkelanjutan untuk karyawan, sangat penting untuk menjaga pertahanan yang kuat terhadap serangan siber. Dengan tetap waspada dan proaktif dalam pendekatan mereka terhadap keamanan siber, bank dapat lebih baik melindungi informasi sensitif pelanggan mereka dan mencegah pelanggaran yang berpotensi menghancurkan. Dalam dunia yang semakin digital, pentingnya langkah-langkah keamanan yang kuat tidak dapat diremehkan, dan bank harus memprioritaskan untuk tetap berada di depan potensi ancaman guna memastikan keamanan dan kepercayaan klien mereka.

Penilaian dan audit keamanan secara berkala

Dapat membantu bank mengidentifikasi kerentanan dalam sistem dan proses mereka, memungkinkan mereka untuk mengatasi kelemahan sebelum dapat

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

dieksploitasi oleh penjahat siber. Selain itu, menetapkan protokol respons insiden yang jelas dan mengujinya secara teratur dapat membantu bank merespons dengan cepat dan efektif jika terjadi pelanggaran. Dengan terus mengevaluasi dan, bank dapat melindungi diri mereka sendiri dan pelanggan mereka dengan lebih baik dari ancaman yang terus berkembang yang ditimbulkan

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

oleh pelaku jahat. Pada akhirnya, berinvestasi dalam praktik keamanan siber yang kuat bukan hanya merupakan persyaratan regulasi bagi bank, tetapi juga komponen penting dalam menjaga reputasi yang baik dan mendapatkan kepercayaan klien mereka.

Ini sangat penting di era digital saat ini, di mana serangan siber semakin canggih dan umum terjadi. Bank harus tetap waspada dan proaktif dalam melindungi sistem dan data mereka dari potensi pelanggaran. Salah satu cara untuk meningkatkan keamanan siber adalah dengan menerapkan otentikasi multi-faktor untuk transaksi perbankan online, yang menambahkan lapisan perlindungan ekstra terhadap akses tidak sah. Secara teratur memperbarui perangkat lunak dan tambalan keamanan adalah praktik penting lainnya untuk mencegah kerentanan yang dapat dieksploitasi oleh peretas. Selain itu, melakukan audit keamanan secara rutin dan pengujian penetrasi dapat membantu mengidentifikasi titik-titik lemah dalam sistem sebelum dapat dieksploitasi. Dengan tetap waspada terhadap potensi ancaman dan terus meningkatkan langkah-langkah keamanan mereka, bank dapat memastikan keselamatan dan keamanan informasi keuangan klien mereka. Ini tidak hanya membantu menjaga kepercayaan dan loyalitas pelanggan mereka tetapi juga melindungi reputasi bank di pasar yang semakin kompetitif.

Perencanaan respons insiden dan pemulihan bencana

Juga merupakan komponen penting dari strategi keamanan siber yang komprehensif untuk bank. Dalam hal terjadi pelanggaran keamanan atau serangan siber, memiliki rencana respons insiden yang terdefinisi dengan baik dapat membantu meminimalkan dampak dan memastikan respons yang cepat dan efektif. Ini termasuk dengan jelas menguraikan peran dan tanggung jawab, menetapkan protokol komunikasi, dan menerapkan langkah-langkah untuk menahan dan mengurangi kerusakan. Demikian pula, perencanaan pemulihan bencana melibatkan pembuatan cadangan data dan sistem yang kritis, serta mengembangkan prosedur untuk memulihkan operasi dalam hal terjadinya peristiwa bencana. Dengan secara proaktif mempersiapkan potensi insiden keamanan, bank dapat meminimalkan waktu henti, mengurangi kerugian finansial, dan melindungi reputasi mereka.di tengah kesulitan. Selain itu, bank harus secara teratur menguji dan memperbarui rencana respons insiden dan pemulihan bencana mereka untuk memastikan rencana tersebut tetap efektif di tengah lanskap ancaman yang terus berkembang. Melatih staf tentang protokol dan prosedur yang tepat juga sangat penting untuk memastikan respons yang cepat dan efisien terhadap setiap insiden keamanan. Dengan berinvestasi dalam langkah-langkah keamanan yang kuat dan tetap waspada, bank dapat mempertahankan kepercayaan dan keyakinan pelanggan dalam kemampuan mereka untuk melindungi aset dan informasi mereka. Pada akhirnya, perencanaan dan persiapan yang proaktif adalah kunci untuk berhasil menghadapi tantangan lanskap keamanan siber saat ini.

Kerangka Kepatuhan dan Regulasi

Tinjauan tentang regulasi dan pedoman untuk manajemen risiko siber dalam perbankan digital

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Kepatuhan terhadap kerangka regulasi sangat penting bagi bank untuk memastikan mereka memenuhi standar yang diperlukan untuk manajemen risiko siber dalam perbankan digital. Regulasi seperti pedoman FFIEC dan persyaratan GDPR menguraikan langkah- langkah spesifik yang harus diambil oleh lembaga keuangan untuk melindungi data pelanggan dan mencegah ancaman siber. Dengan tetap mengikuti perkembangan regulasi ini dan menerapkan kontrol yang diperlukan, bank dapat menunjukkan komitmen mereka

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

terhadap kepatuhan dan mengurangi risiko denda yang mahal akibat ketidakpatuhan. Selain itu, secara teratur meninjau dan memperbarui kebijakan serta prosedur untuk menyesuaikan dengan perubahan regulasi sangat penting untuk mempertahankan posisi keamanan siber yang kuat di tengah ancaman yang terus berkembang. Misalnya, sebuah bank dapat secara rutin melakukan audit internal dan pengujian penetrasi untuk memastikan sistem mereka aman dan sesuai dengan peraturan. Mereka juga dapat berinvestasi dalam teknologi keamanan siber canggih seperti enkripsi dan autentikasi multi-faktor untuk lebih melindungi data pelanggan dari serangan siber. Dengan tetap proaktif dan waspada dalam langkah- langkah keamanan siber mereka, bank tidak hanya dapat melindungi informasi sensitif pelanggan mereka tetapi juga menjaga reputasi dan aset keuangan mereka. Penting bagi organisasi untuk memprioritaskan keamanan siber sebagai perhatian utama dan mengalokasikan sumber daya dengan tepat untuk tetap unggul dalam menghadapi potensi ancaman. Dengan mengambil langkah-langkah proaktif ini, bank dapat menunjukkan komitmen terhadap praktik terbaik keamanan siber dan mempertahankan kepercayaan pelanggan mereka di dunia yang semakin digital.

Tantangan kepatuhan yang dihadapi oleh bank digital

Termasuk menavigasi persyaratan regulasi yang kompleks, memastikan privasi dan perlindungan data, serta mengelola risiko vendor pihak ketiga. Tantangan-tantangan ini mengharuskan bank digital untuk terus beradaptasi dan mengembangkan strategi keamanan siber mereka agar tetap patuh dan aman. Selain itu, sifat industri perbankan digital yang bergerak cepat berarti bahwa persyaratan kepatuhan terus berubah, sehingga penting bagi bank untuk tetap terinformasi dan mengikuti perkembangan regulasi terbaru. Gagal memenuhi standar kepatuhan dapat mengakibatkan denda besar, konsekuensi hukum, dan kerusakan pada reputasi bank. Oleh karena itu, bank digital harus memprioritaskan upaya kepatuhan bersamaan dengan langkah-langkah keamanan siber mereka untuk memastikan keselamatan dan kepercayaan pelanggan mereka. Dengan berinvestasi dalam sistem keamanan siber yang kuat dan tetap berada di depan perubahan regulasi, bank dapat melindungi data mereka dan melindungi dari potensi pelanggaran atau serangan. Audit dan penilaian rutin dapat membantu mengidentifikasi setiap kerentanan dan memastikan bahwa bank tetap mematuhi standar industri. Pada akhirnya, menjaga fokus yang kuat pada keamanan siber dan kepatuhan sangat penting bagi bank digital untuk berkembang dalam lanskap keuangan yang terus berubah dan mempertahankan kepercayaan pelanggan mereka.

Praktik terbaik untuk tetap mematuhi peraturan

Termasuk melakukan penilaian risiko secara berkala, tetap mendapatkan informasi tentang pembaruan regulasi, dan menerapkan sistem manajemen kepatuhan yang kuat. Banks should also establish clear policies and procedures for data protection and regularly train employees on cybersecurity best practices (Hennie & Sonja, 2009) . Selain itu, berkolaborasi dengan para ahli industri dan berpartisipasi dalam inisiatif berbagi informasi dapat membantu bank tetap unggul

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

dalam menghadapi ancaman yang muncul dan memastikan mereka memenuhi semua persyaratan kepatuhan yang diperlukan. Dengan mengambil pendekatan proaktif terhadap kepatuhan dan keamanan siber, bank digital tidak hanya dapat melindungi data dan reputasi mereka tetapi juga membangun kepercayaan dengan pelanggan mereka dan mempertahankan keunggulan kompetitif di pasar. Dalam lanskap digital yang berkembang pesat saat ini, sangat penting bagi bank untuk memprioritaskan langkah-langkah keamanan

siber guna melindungi informasi sensitif pelanggan mereka. Menerapkan otentikasi multi- faktor dan protokol enkripsi dapat lebih meningkatkan keamanan platform online mereka dan mencegah akses tidak sah ke data. Dengan berinvestasi dalam langkah-langkah keamanan siber yang kuat dan mengikuti standar industri, bank digital dapat menciptakan lingkungan perbankan yang aman dan dapat diandalkan bagi pelanggan mereka, yang pada akhirnya akan mengarah pada kesuksesan jangka panjang dan pertumbuhan di dunia digital. sektor perbankan.

Studi Kasus Manajemen Risiko Siber yang Sukses
Contoh bank digital yang telah berhasil mengelola risiko siber

Termasuk Bank XYZ dan Bank ABC. Bank XYZ menerapkan kerangka kerja keamanan siber yang komprehensif yang mencakup audit keamanan reguler, program pelatihan karyawan, dan pemantauan terus-menerus terhadap sistem mereka untuk setiap potensi ancaman. As a result, they have successfully thwarted numerous cyber attacks and maintained the trust of their customers (Kemas & Achmad, 2024) . Di sisi lain, Bank ABC mengalami pelanggaran data di masa lalu karena langkah-langkah keamanan yang tidak memadai. Namun, mereka dengan cepat belajar dari kesalahan mereka dan berinvestasi dalam teknologi keamanan siber mutakhir untuk mencegah insiden di masa depan. Pendekatan proaktif ini tidak hanya membantu mereka mendapatkan kembali kepercayaan pelanggan mereka tetapi juga memposisikan mereka sebagai pemimpin dalam manajemen risiko siber di industri perbankan digital. Misalnya, XYZ Corporation menerapkan perangkat lunak deteksi ancaman waktu nyata yang secara konstan memindai jaringan mereka untuk setiap aktivitas mencurigakan. Ini telah memungkinkan mereka untuk mendeteksi dan menetralkan ancaman sebelum dapat menyebabkan kerusakan, memastikan keamanan data mereka dan privasi pelanggan mereka. Sebaliknya, pelanggaran data di ABC Bank disebabkan oleh protokol keamanan yang sudah usang yang membuat mereka rentan terhadap serangan. Dengan meningkatkan langkah-langkah keamanan siber mereka dan berinvestasi dalam audit keamanan reguler, mereka berhasil memperkuat pertahanan mereka dan mencegah pelanggaran di masa depan, yang pada akhirnya mendapatkan kepercayaan pelanggan mereka dan melindungi informasi sensitif mereka. Dengan langkah-langkah baru ini, ABC Bank sekarang dapat fokus pada memberikan pengalaman perbankan yang aman dan andal bagi pelanggan mereka, mengetahui bahwa data mereka aman dari ancaman siber. Pendekatan proaktif yang diambil oleh Corporation dan ABC Bank menyoroti pentingnya tetap berada di depan potensi risiko keamanan di era digital saat ini.

Dampak manajemen risiko siber terhadap posisi keamanan keseluruhan bank digital

Selain melindungi data pelanggan, penerapan strategi manajemen risiko siber yang kuat juga telah berdampak positif pada posisi keamanan keseluruhan bank digital. Dengan terus-menerus memantau dan memperbarui pertahanan mereka, bank-bank ini lebih siap untuk mendeteksi dan merespons ancaman yang

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

muncul secara real-time. Pendekatan proaktif ini tidak hanya membantu mencegah potensi pelanggaran, tetapi juga memungkinkan bank digital untuk tetap selangkah lebih maju dari penjahat siber. Akibatnya, pelanggan dapat merasa yakin akan keamanan informasi keuangan mereka dan percaya bahwa bank mereka mengambil langkah-langkah yang diperlukan untuk melindungi data mereka. Meskipun benar

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

bahwa strategi manajemen risiko siber yang kuat dapat meningkatkan posisi keamanan, penting untuk dicatat bahwa tidak ada sistem yang sepenuhnya bebas dari kesalahan dan ancaman siber terus berkembang. Selain itu, efektivitas strategi-strategi ini dapat terbatas oleh kesalahan manusia atau kerentanan dalam sistem pihak ketiga. Oleh karena itu, sangat penting bagi bank digital untuk terus memantau dan memperbarui langkah-langkah keamanan mereka agar dapat beradaptasi dengan ancaman dan kerentanan baru. Penilaian dan audit keamanan secara berkala dapat membantu mengidentifikasi dan mengatasi kelemahan dalam sistem sebelum dapat dieksploitasi oleh penjahat siber. Dengan tetap proaktif dan waspada dalam pendekatan mereka terhadap keamanan siber, bank digital dapat meminimalkan risiko dan melindungi baik pelanggan mereka maupun reputasi mereka dalam jangka panjang. Pada akhirnya, berinvestasi dalam manajemen risiko siber yang kuat bukan hanya merupakan pengeluaran yang diperlukan, tetapi juga aspek penting dalam menjaga kepercayaan dan loyalitas di antara pelanggan di dunia perbankan yang semakin digital.

Kesimpulan

Secara keseluruhan, jelas bahwa bank digital harus tetap berada di depan dalam hal keamanan siber untuk melindungi informasi sensitif pelanggan mereka dan menjaga kredibilitas mereka di industri. Dengan tetap mendapatkan informasi tentang ancaman terbaru, berkolaborasi dengan institusi lain, dan memprioritaskan langkah-langkah keamanan, bank digital dapat secara efektif melawan ancaman siber dan melindungi reputasi mereka. Sangat penting bagi bank digital untuk terus berinvestasi dalam protokol keamanan yang kuat dan tetap waspada guna mengurangi risiko yang ditimbulkan oleh penjahat siber. Kesimpulannya, keamanan siber harus tetap menjadi prioritas utama bagi bank digital untuk memastikan keselamatan dan kepercayaan pelanggan mereka di dunia yang semakin digital. Dengan menerapkan audit keamanan secara rutin dan melakukan penilaian risiko yang menyeluruh, bank digital dapat tetap selangkah lebih maju dari potensi serangan siber. Selain itu, memberikan pelatihan berkelanjutan kepada karyawan tentang praktik terbaik keamanan siber dapat membantu menciptakan budaya kesadaran keamanan di dalam organisasi. Pada akhirnya, dengan mengambil langkah-langkah proaktif dan tetap proaktif, bank digital dapat melindungi informasi sensitif pelanggan mereka dan mempertahankan keunggulan kompetitif mereka di lanskap digital yang terus berkembang.

Rekomendasi untuk meningkatkan manajemen risiko siber di industri perbankan digital

Termasuk menerapkan otentikasi multi-faktor untuk semua akun pelanggan, secara teratur memperbarui perangkat lunak dan sistem untuk menambal kerentanan, serta menetapkan rencana respons jika terjadi pelanggaran keamanan. Selain itu, berkolaborasi dengan para ahli industri dan berbagi intelijen ancaman juga dapat meningkatkan pertahanan bank digital terhadap ancaman siber. Dengan terus-menerus menyesuaikan dan meningkatkan langkah-langkah

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 15 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

keamanan siber mereka, bank digital dapat membangun kepercayaan dengan pelanggan mereka dan melindungi reputasi mereka di dunia yang semakin digital. Selain itu, melakukan audit keamanan secara berkala dan pengujian penetrasi dapat membantu mengidentifikasi kelemahan dalam sistem sebelum dapat dieksploitasi oleh penjahat siber. Penting juga bagi bank digital untuk berinvestasi dalam program pelatihan dan kesadaran

karyawan guna memastikan bahwa semua anggota staf memahami pentingnya keamanan siber dan dilengkapi untuk menangani potensi ancaman. Dengan mengambil langkah-langkah proaktif ini, bank digital dapat tetap unggul dalam menghadapi ancaman siber dan menjaga lingkungan yang aman untuk informasi keuangan pelanggan mereka.

Arah penelitian masa depan

Di bidang keamanan siber untuk bank digital mungkin termasuk mengeksplorasi penggunaan kecerdasan buatan dan algoritma pembelajaran mesin untuk mendeteksi dan mencegah serangan siber secara waktu nyata. Selain itu, studi lebih lanjut dapat menyelidiki efektivitas teknologi blockchain dalam meningkatkan keamanan sistem perbankan digital. Dengan tetap mengikuti perkembangan terbaru dalam teknologi keamanan siber dan terus meningkatkan pertahanan mereka, bank digital dapat lebih baik melindungi pelanggan mereka dan mempertahankan reputasi mereka sebagai lembaga keuangan yang aman. Selain itu, para peneliti juga dapat menyelidiki potensi kerentanan yang ditimbulkan oleh teknologi baru seperti komputasi kuantum dan perangkat IoT dalam sistem perbankan digital. Memahami dan menangani potensi ancaman ini akan sangat penting untuk tetap unggul dari para penjahat siber. Dengan berinvestasi dalam penelitian dan pengembangan mutakhir, bank digital dapat memastikan mereka siap menghadapi lanskap ancaman keamanan siber yang terus berkembang dan mempertahankan kepercayaan pelanggan mereka. Pada akhirnya, pendekatan proaktif terhadap penelitian keamanan siber akan sangat penting dalam melindungi masa depan perbankan digital.

Daftar Pustaka

Alice, & Alexis. (2002). *Risk management guide for information technology systems.*

Hennie, & Sonja. (2009). *Analyzing banking risk.*

Kemas, & Achmad. (2024). *Information Security Awareness Analysis on Digital Bank Customer Using Analytic Hierarchy Process: Case Study at XYZ Application from Bank ABC.*

Samuel, Adedolapo, Odunayo, Abimbola, & Sarah. (2023). *Cybersecurity risk assessment in banking: methodologies and best practices.*

Thomas, & Phil. (2016). *Financial data breaches in the US retail economy: Restoring confidence in information technology security standards.*