Jurnal Sinabis
https://jsinabis.upnjatim.ac.id/index.php/jsinabis
ISSN (Online): XXXX-XXX
Volume 1 Nomor 6 Desember 2025

Analisis Peran Cybersecurity Guna Menghadapi Ancaman Cybercrime: Studi Kasus pada PT. Bank Pembangunan Daerah Jawa Timur Tbk

Richard Danuarta & Nurul Azizah
Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia
21042010275@student.upnjatim.ac.id

ABSTRAK

Perkembangan teknologi digital telah membawa banyak manfaat bagi sektor perbankan, namun juga meningkatkan risiko kejahatan siber yang semakin kompleks. Kejahatan siber seperti phishing, malware, ransomware, dan pencurian data dapat mengancam reputasi, stabilitas keuangan, dan kepercayaan nasabah terhadap bank. Oleh karena itu, keamanan siber menjadi krusial bagi bank untuk melindungi aset dan data nasabah. Penelitian ini bertujuan untuk menganalisis efektivitas strategi keamanan siber yang diterapkan oleh PT. Bank Pembangunan Daerah Jawa Timur Tbk. (Bank Jatim) dalam menghadapi ancaman kejahatan siber. Melalui metode studi kasus dengan pendekatan kualitatif, penelitian ini mengkaji implementasi keamanan siber di Bank Jatim dengan mengumpulkan data melalui wawancara, observasi, dan studi dokumentasi. Hasil penelitian menunjukkan bahwa Bank Jatim telah membangun sistem keamanan siber yang kuat, ditandai dengan tingginya kesadaran karyawan akan pentingnya keamanan siber dan penerapan kerangka kerja keamanan siber yang komprehensif. Bank Jatim telah berinvestasi dalam infrastruktur keamanan yang memadai, termasuk firewall, sistem deteksi intrusi, dan perangkat lunak antivirus, serta membentuk tim khusus untuk memantau dan merespons ancaman siber. Meskipun demikian, Bank Jatim tetap menghadapi tantangan dalam menghadapi serangan siber yang terus berkembang. Penelitian ini menyoroti pentingnya penerapan kerangka kerja keamanan siber yang terstruktur dan berkelanjutan bagi bank untuk memitigasi risiko dan melindungi aset serta data nasabah dari ancaman kejahatan siber.

Kata Kunci: Teknologi, Keamanan Siber, Kejahatan Siber

ABSTRACT

The development of digital technology has brought many benefits to the banking sector, but it also increases the risk of increasingly complex cybercrime. Cybercrimes such as phishing, malware, ransomware, and data theft can threaten a bank's reputation, financial stability, and customer trust. Therefore, cybersecurity is crucial for banks to protect customer assets and data. This study aims to analyze the effectiveness of cybersecurity strategies implemented by PT Bank Pembangunan Daerah Jawa Timur Tbk (Bank Jatim) in dealing with the threat of cybercrime. Through a case study method with a qualitative approach, this research examines the implementation of cybersecurity at Bank Jatim by collecting data through interviews, observations, and documentation studies. The results show that Bank Jatim has built a strong cybersecurity system, characterized by high employee awareness of the importance of cybersecurity and the implementation of a comprehensive cybersecurity framework. Bank Jatim has invested in adequate security infrastructure, including firewalls, intrusion detection systems, and antivirus software, and established a dedicated team to monitor and respond to cyber threats. Nonetheless, Bank Jatim still faces challenges in dealing with evolving cyber-attacks. This research highlights the importance of implementing a structured and sustainable cybersecurity framework for banks to mitigate risks and protect assets and customer data from cybercrime threats.

Keywords: Technology, Cyber Security, Cybercrime.

PENDAHULUAN

Perkembangan teknologi digital yang cepat telah memberikan banyak manfaat bagi sektor perbankan, tetapi juga memunculkan risiko keamanan siber yang lebih rumit dan berbahaya. Lembaga keuangan, khususnya bank-bank di Indonesia, sangat menderita akibat kejahatan siber. Reputasi, stabilitas keuangan, dan bahkan kepercayaan nasabah terhadap bank dapat terancam oleh berbagai taktik kejahatan siber, termasuk phishing, malware, serangan ransomware, dan pencurian data. Tujuan utama dari kejahatan dunia maya, khususnya di industri keuangan, adalah untuk mendapatkan keuntungan pribadi yang tidak sah. Informasi bank atau nasabah yang sensitif dapat bocor melalui kesalahan internal atau peretasan langsung, yang dikenal sebagai pembobolan data. Pencurian data sensitif, kerugian moneter, dan kerusakan reputasi adalah hasil yang mungkin terjadi dari serangan ini. (Fitria, 2023).

Maka dari itu, Pemerintah Indonesia membuat UU *cybercrime* dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dirancang untuk menyelaraskan instrumen hukum nasional dengan instrumen hukum internasional yang mengatur teknologi informasi. *Cybersecurity* memainkan peran penting dalam memastikan industri perbankan bertahan dalam menghadapi tantangan ini. Keamanan siber terdiri dari pendekatan holistik yang mencakup pencegahan, deteksi, reaksi, dan pemulihan terhadap insiden keamanan siber, dan tidak hanya terbatas pada perlindungan sistem dan jaringan (Sibero, 2021). Kerangka kerja yang sistematis, seperti *NIST Cybersecurity Framework* (CSF) atau ISO 27001, yang disesuaikan dengan persyaratan dan fitur perbankan diperlukan untuk penerapan keamanan siber yang efektif (Rahman, Fachrurozi, & Safitri, 2024)

Peraturan dari Otoritas Jasa Keuangan (OJK), seperti Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, yang mengamanatkan bank untuk membangun sistem pengendalian internal yang memadai dalam mengelola risiko teknologi informasi, termasuk risiko keamanan siber, semakin menyoroti pentingnya keamanan siber di sektor perbankan. Penerapan keamanan siber yang tidak memadai dapat menyebabkan kerugian finansial, denda dari pemerintah, dan penurunan kepercayaan masyarakat terhadap bank.

Studi kasus PT. Bank Pembangunan Daerah Jawa Timur, Tbk. (Bank Jatim) memberikan gambaran menarik tentang bagaimana keamanan siber harus diterapkan dalam menghadapi ancaman kejahatan siber dalam proses bisnis. Sebagai salah satu BPD terbesar di Indonesia, Bank Jatim menghadapi kesulitan yang unik dalam menjaga integritas sistem dan keamanan data nasabah saat menjalani transisi digital yang berkelanjutan.

Penelitian ini bertujuan untuk menguji taktik dan langkah-langkah yang diterapkan oleh Bank Jatim untuk memitigasi risiko keamanan siber, menilai keefektifannya dalam mengatasi berbagai bentuk kejahatan siber serta diharapkan dapat memberikan ringkasan menyeluruh tentang pentingnya keamanan siber bagi BPD dan berfungsi sebagai panduan untuk mening-katkan protokol keamanan informasi di seluruh sektor perbankan.

METODE PELAKSANAAN

Penelitian kualitatif dengan metode studi kasus ini akan dilakukan di PT. Bank Pembangunan Daerah Jawa Timur Tbk. (Bank Jatim) untuk mendalami implementasi keamanan

siber dalam menghadapi ancaman kejahatan siber. Data primer akan dikumpulkan melalui wawancara mendalam dengan narasumber kunci seperti manajer TI dan staf keamanan siber, observasi langsung proses implementasi keamanan siber, dan studi dokumentasi seperti kebijakan dan prosedur terkait.

HASIL DAN PEMBAHASAN

Cybersecurity

Keamanan siber adalah bidang yang terus berkembang dan sangat penting di era digital saat ini. Sederhananya, keamanan siber mengacu pada praktik melindungi sistem, jaringan, program, dan data dari serangan siber. Serangan ini dapat terjadi dalam berbagai bentuk, termasuk pencurian data, malware, ransomware, phishing, dan serangan *Denial-of-Service* (DoS). Tujuan utama keamanan siber adalah untuk memastikan *Confidentiality* (kerahasiaan), *Intergrity* (Integritas), dan *Availability* (Ketersediaan) informasi, yang sering disebut sebagai "CIA triad" (Stallings & Brown,2014).

Keamanan siber melibatkan berbagai teknologi, proses, dan praktik terbaik untuk mencapai tujuan-tujuan ini, termasuk firewall, enkripsi, otentikasi dua faktor, dan pelatihan kesadaran keamanan. Selain itu, keamanan siber juga mencakup aspek manajemen risiko, pemulihan bencana, dan kepatuhan terhadap standar dan peraturan yang relevan. Dengan meningkatnya ketergantungan pada teknologi dan semakin canggihnya ancaman siber, keamanan siber menjadi semakin penting bagi individu, organisasi, dan pemerintah di seluruh dunia.

Cybercrime

Cybercrime menggunakan Teknologi informasi dan komunikasi sebagai senjata atau target. Fenomena ini berkembang dengan cepat seiring dengan kemajuan teknologi dan meningkatnya aktivitas internet. Kejahatan siber telah berubah secara dramatis selama lima tahun terakhir, baik dari segi kecanggihan maupun jenis serangannya (Sulistyowati & Solichin, 2020). Phishing, serangan ransom-ware, pencurian data, dan serangan Distributed Denial of Service (DDoS) adalah beberapa dari sekian banyak bentuk kejahatan siber yang lazim terjadi saat ini.

Phishing adalah tindakan penipuan dengan menyamar sebagai sumber yang dapat dipercaya untuk mendapatkan informasi pribadi, termasuk nomor kartu kredit dan kata sandi. Ransomware mengenkripsi data targetnya dan meminta uang tebusan untuk membukanya. Pencurian data merugikan banyak orang dan bisnis. Dengan membebani sistem atau jaringan dengan data, serangan DDoS berusaha membuat sistem atau jaringan tersebut tidak dapat beroperasi.

Hasil penelitian

Dalam penelitian ini menunjukkan bahwa Bank Jatim telah mengembangkan sistem *cybersecurity* yang kuat, seperti yang ditunjukkan oleh kesadaran yang tinggi di antara anggota stafnya. Karena bank telah secara konsisten berinvestasi dalam pelatihan keamanan siber dan inisiatif kesadaran, mayoritas pekerja menunjukkan pemahaman yang kuat tentang perlunya keamanan siber dalam melindungi aset bank dan data pelanggan.

Infrastruktur *cybersecurity* yang kuat dari Bank Jatim, yang terdiri dari firewall, intrution detection system, dan antivirus software yang bekerja sama untuk menghentikan dan mengurangi serangan siber, merupakan indikasi lain dari dedikasi perusahaan terhadap keamanan siber. Protokol

keamanan bank semakin diperkuat dengan pemantauan konstan dan respons ancaman yang disediakan oleh tim *cybersecurity* khusus.

Implementasi *Framework Cybersecurity*

Komitmen Bank Jatim terhadap keamanan siber terlihat dari penerapan kerangka kerja yang komprehensif, yang sesui dengan standar yang diakui secara global seperti *NIST Framework Cybersecurity* atau ISO 27001. Kerangka kerja ini, yang disesuaikan dengan konteks spesifik bank, memberikan pendekatan terstruktur untuk mengelola dan memitigasi risiko siber. Kerangka kerja ini mencakup lima fungsi inti:

a. *Identify:* Informasi pelanggan, sistem perbankan utama, dan infrastruktur jaringan adalah beberapa aset penting yang dimiliki oleh Bank Jatim. Mereka secara teratur mengevaluasi penilaian risiko agar tetap berada di barisan depan ketika terdapat ancaman yang terus muncul.
b. *Protect:* Dengan menggunakan *firewall, intrusion* deteksi intrusi, enkripsi data, dan otentikasi dua faktor, Bank Jatim memiliki sistem pertahanan berlapis. Elemen penting dari rencana perlindungan mereka juga peraturan keamanan yang ketat dan pelatihan karyawan.
c. *Detect:* Untuk memungkinkan reaksi dan mitigasi yang cepat, Bank Jatim memiliki sistem pemantauan yang canggih untuk secara instan menemukan aktivitas yang meragukan dan kemungkinan cyberattack.
d. *Respond:* Untuk meminimalkan kerusakan dan segera melanjutkan operasi reguler, *Cyber Security Incident Response Team* (CSIRT) merespons insiden keamanan sesuai dengan protokol yang telah ditetapkan.
e. *Recover:* Untuk menjamin kelangsungan bisnis jika terjadi *cybercrime* atau gangguan sistem, Bank Jatim memiliki rencana pemulihan bencana yang kuat. Hal ini meliputi proses untuk memulihkan layanan dengan cepat, sistem alternatif, dan backup data.

Diskusi dengan Badan Intelejen Negara Jawa Timur:

Penyelenggaraan diskusi panel dengan Badan Intelijen Negara (BIN) Jawa Timur merupakan langkah strategis yang menunjukkan komitmen kuat Bank Jatim dalam meningkatkan keamanan siber dan mencegah kejahatan keamanan data. Diskusi ini tidak hanya menjadi forum pertukaran informasi, tetapi juga wahana kolaborasi yang memberikan beragam manfaat signifikan bagi Bank Jatim.

a. Peningkatan Pemahaman: Diskusi panel menjadi platform efektif untuk berbagi pengetahuan dan wawasan terkini terkait lanskap ancaman siber yang terus berkembang. Melalui diskusi interaktif, Bank Jatim dapat memperoleh informasi berharga mengenai tren ancaman siber, modus operandi kejahatan siber yang semakin canggih, serta strategi pencegahan yang efektif dari para pakar dan praktisi di bidang keamanan siber, termasuk dari BIN Jawa Timur.
b. Penguatan Koordinasi: Diskusi panel ini memfasilitasi terjalinnya kerja sama dan koordinasi yang lebih erat antara Bank Jatim dan BIN Jawa Timur dalam menghadapi ancaman keamanan siber. Sinergi antara kedua institusi ini sangat krusial dalam upaya proaktif untuk mencegah dan menanggulangi kejahatan siber yang semakin kompleks. Kolaborasi ini dapat meliputi

pertukaran informasi intelijen, pelatihan bersama, serta pengembangan strategi keamanan siber yang komprehensif.

c. Peningkatan Kesiapsiagaan: Dengan memperoleh informasi intelijen dan wawasan strategis dari BIN Jawa Timur, Bank Jatim dapat meningkatkan kesiapsiagaan dalam menghadapi potensi serangan siber. Akses terhadap informasi terkini mengenai ancaman siber, kerentanan sistem, dan modus operandi kejahatan siber memungkinkan Bank Jatim untuk mengambil langkah-langkah pencegahan yang tepat dan merespons insiden keamanan secara cepat dan efektif.
d. Pengembangan Strategi: Diskusi panel dengan BIN Jawa Timur juga dapat memberikan masukan yang berharga bagi Bank Jatim dalam mengembangkan strategi keamanan siber yang lebih komprehensif dan adaptif. Melalui diskusi dan pertukaran pandangan dengan para ahli di bidang keamanan siber, Bank Jatim dapat mengidentifikasi area yang perlu ditingkatkan dalam sistem keamanan mereka dan merumuskan strategi yang lebih efektif untuk memitigasi risiko siber.

Dengan demikian, diskusi panel dengan BIN Jawa Timur merupakan investasi strategis bagi Bank Jatim dalam meningkatkan postur keamanan siber dan melindungi aset serta data nasabah dari ancaman kejahatan siber yang terus berkembang.

Upaya Pencegahan Cybercrime Lainnya:

Bank Jatim menyadari bahwa upaya pencegahan *cybercrime* memerlukan pendekatan yang *multi-faceted* dan berkelanjutan. Oleh karena itu, selain menyelenggarakan diskusi panel dengan BIN Jawa Timur, Bank Jatim juga aktif melaksanakan berbagai inisiatif lain untuk memperkuat postur keamanan siber dan melindungi aset serta data nasabah dari ancaman kejahatan siber.

a. Edukasi dan Pelatihan: Bank Jatim secara konsisten memberikan edukasi dan pelatihan keamanan siber kepada seluruh karyawan secara berkala. Program pelatihan ini didesain untuk meningkatkan kesadaran dan pengetahuan karyawan mengenai berbagai jenis ancaman siber, modus operandi kejahatan siber, serta strategi pencegahan yang efektif. Dengan meningkatkan literasi keamanan siber di seluruh tingkatan organisasi, Bank Jatim berupaya untuk membangun "*human firewall"* yang tangguh dalam mencegah serangan siber, terutama yang menargetkan aspek human error seperti phishing dan social engineering.
b. Simulasi Serangan Siber: Untuk menguji keefektifan sistem keamanan siber dan melatih tim *Cyber Security Incident Response Team (*CSIRT) dalam menangani insiden keamanan, Bank Jatim secara rutin menyelenggarakan simulasi serangan siber. Simulasi ini mensimulasikan berbagai skenario serangan siber yang realistis, memungkinkan tim CSIRT untuk mempraktikkan prosedur respons insiden, mengidentifikasi kerentanan sistem, dan meningkatkan kemampuan dalam memitigasi dampak serangan siber. Melalui simulasi ini, Bank Jatim dapat mengevaluasi kesiapan dalam menghadapi serangan siber yang sebenarnya dan melakukan perbaikan yang diperlukan untuk memperkuat sistem keamanan siber.
c. Kerja Sama dengan Pihak Eksternal: Bank Jatim juga aktif membangun kerja sama dengan pihak eksternal yang memiliki keahlian di bidang keamanan siber, seperti

konsultan keamanan siber dan penyedia layanan keamanan terkelola (*Managed Security Service Provider/MSSP*). Kerja sama ini bertujuan untuk memperoleh pendampingan dan dukungan dalam meningkatkan keamanan siber, meliputi penilaian kerentanan sistem, implementasi teknologi keamanan terkini, dan manajemen risiko siber. Dengan memanfaatkan keahlian dan sumber daya dari pihak eksternal, Bank Jatim dapat memperkuat sistem keamanan siber dan meningkatkan kemampu-an dalam menghadapi ancaman kejahatan siber yang semakin canggih.

Upaya-upaya pencegahan *cybercrime* yang dilakukan oleh Bank Jatim ini menunjukkan komitmen yang kuat dalam menjaga keamanan aset dan data nasabah. Dengan menerapkan pendekatan yang komprehensif dan berkelanjutan, Bank Jatim berupaya untuk meminimalkan risiko kejahatan siber dan memastikan kelangsungan operasional bisnis di era digital yang penuh dengan tantangan.

KESIMPULAN

Studi ini melihat nilai keamanan siber dalam mengatasi ancaman kejahatan siber yang meningkat di era digital, terutama untuk lembaga keuangan seperti Bank Jatim. Dengan menerapkan langkah-langkah komprehensif, seperti meningkatkan kesadaran karyawan, membangun infrastruktur yang solid, dan menerapkan kerangka kerja keamanan siber yang terstruktur berdasarkan standar internasional seperti NIST CSF atau ISO 27001, Bank Jatim telah menunjukkan komitmen yang kuat terhadap keamanan siber. Namun, masalah kejahatan siber masih terus berlanjut, menggaris bawahi perlunya peningkatan dan modifikasi taktik keamanan siber yang berkelanjutan. Studi ini memberikan wawasan kepada sektor perbankan untuk memperkuat pertahanan terhadap ancaman kejahatan siber dan memberikan ringkasan tentang upaya Bank Jatim untuk menjaga keamanan sistem dan data nasabah.

DAFTAR PUSTAKA

Sulistyowati, D. A., & Solichin, A. (2020). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Konstituen: Jurnal Ilmu Pemerintahan, 7*(3), 527–540.

Rahman, Fachrurozi, & Safitri. (2024). Urgensi Penerapan ISO 27001 Pada Perbankan Syariah di Indonesia. *STAI Bina Madani, 7*(1), 71-83

Maulidah Narastri.2020."Financial Technology (Fintech) di Indonesia Ditinjau Dari Perspektif Islam. *"Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE) 2, No.2*(2020): 155-170.

Fitri, J. (2021). “Pengaruh Internet Banking dan Cyber Crime Terhadap Kepercayaan Nasabah di Perbankan Syariah (Studi Pada Bank Syariah Mandiri Tapak Tuan),” *skripsi* UIN Ar Raniry, tersedia (https://repository.arraniry.ac.id/id/eprint/21335/)

Rudiatno, & Cheryta, A. M. (2022). Evaluasi Kebijakan Cyber Security Sektor Perbankan Bank BTN Cabang Surabaya. *e-Jurnal Apresiasi Ekonomi, 10*(03). 321-331.

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Jurnal Risalah Hukum, 17*(2), 98-107.

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. *Jurnal Informatika dan Teknik Elektro Terapan*, 721-730.

Rohmah, R. N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendekia Niaga: Journal of Trade Development and Studies*, *6*(1), 1–11.

Ervina Chintia, R. N. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Education Technology*, *2*(2) ,65-69