Nusantara Journal of Multidisciplinary Science
Vol. 2, No. 1, Januari 2024
Hal 228-232
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Perkembangan Management Sekuriti Di PT Bank Central Asia (BCA)

Ahmad Sofiyan[1], Khoiridha Askiyyah[2], Ulfa Amelia[3], Fried Sinlae[4]
[1,2,3,4] Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Article Info

Article history:

Received Januari 1, 2024
Revised Januari 2, 2024
Accepted Januari 12, 2024

Keywords:

Keamanan Informasi,
Manajemen Keamanan,
Tantangan Keamanan Siber di Indonesia.

Keywords:

Information Security,
Security Management,
Cyber Security Challenges in Indonesia.

ABSTRAK

Dalam era digital yang terus berkembang, keamanan informasi menjadi aspek krusial dalam memastikan kelangsungan dan integritas organisasi. Artikel ini menggambarkan perkembangan manajemen sekuriti di Indonesia, sebuah negara dengan pertumbuhan ekonomi yang pesat dan adopsi teknologi informasi yang signifikan. Dengan latar belakang ini, penelitian ini bertujuan untuk mengeksplorasi evolusi manajemen sekuriti, mengidentifikasi tantangan khusus yang dihadapi oleh organisasi di Indonesia, serta mengevaluasi peluang yang muncul dalam mengelola risiko keamanan informasi.Pemerintah Indonesia telah mengambil langkah-langkah penting dalam menciptakan lingkungan yang aman dan andal, dengan menerapkan peraturan dan standar terkait keamanan informasi. Namun, pelaksanaan manajemen sekuriti di berbagai sektor masih dihadapkan pada sejumlah tantangan, termasuk kompleksitas ancaman siber, kekurangan sumber daya manusia yang terlatih, dan keterbatasan akses terhadap teknologi terkini

ABSTRACT

In the ever-growing digital era, information security has become a crucial aspect in ensuring organizational continuity and integrity. This article describes the development of security management in Indonesia, a country with rapid economic growth and significant adoption of information technology. Against this background, this research aims to explore the evolution of security management, identify specific challenges faced by organizations in Indonesia, and evaluate emerging opportunities in managing information security risks. The Indonesian government has taken important steps in creating a safe and reliable environment , by implementing regulations and standards related to information security. However, the implementation of security management in various sectors is still faced with a number of challenges, including the complexity of cyber threats, a shortage of trained human resources, and limited access to the latest technology

This is an open access article under the CC BY license.

Corresponding Author:

Fried Sinlae
Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya
Jakarta, Indonesia,
Email: fried.sinlae@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Dalam era digital yang semakin berkembang, manajemen keamanan (security management) menjadi suatu aspek yang krusial, terutama bagi lembaga keuangan seperti PT Bank Central Asia (BCA). Bank BCA sebagai salah satu lembaga keuangan terkemuka di Indonesia, dengan kompleksitas operasional dan jumlah transaksi yang tinggi, menempatkan manajemen keamanan sebagai prioritas utama. Penelitian ini akan mengkaji perkembangan manajemen keamanan di Bank BCA, melibatkan tinjauan sejarah, evolusi, dan tantangan terkini yang dihadapi oleh lembaga tersebut.

"Keamanan menjadi elemen kunci dalam operasional perbankan, terutama ketika melibatkan data dan transaksi keuangan pelanggan [1] Manajemen keamanan tidak hanya sekadar perlindungan terhadap serangan siber, tetapi juga mengenai integritas data dan kepercayaan pelanggan. "Dengan berkembangnya teknologi digital, bank-bank dihadapkan pada tantangan baru dalam memastikan keamanan informasi yang disimpan dan diproses [2]. Tantangan ini mencakup serangan siber yang semakin canggih, kebutuhan akan perlindungan data pelanggan, dan peningkatan regulasi terkait privasi. "Manajemen keamanan tidak hanya berfokus pada aspek teknologi, tetapi juga memainkan peran penting dalam pencegahan kriminalitas keuangan seperti pencucian uang dan penipuan [3]. Keberhasilan manajemen keamanan akan berdampak positif pada keamanan ekosistem perbankan secara keseluruhan. Perkembangan manajemen keamanan di lembaga keuangan Indonesia mencerminkan evolusi dari pendekatan tradisional menuju strategi yang lebih proaktif dan adaptif [4]. Sejarah ini dapat memberikan pemahaman tentang bagaimana lembaga keuangan, termasuk Bank BCA, menanggapi perubahan lingkungan keamanan.

Manajemen keamanan berbasis risiko telah menjadi pendekatan yang umum diterapkan oleh bank-bank modern untuk mengidentifikasi dan mengelola ancaman dengan lebih efisien. [5] Implementasi pendekatan ini di Bank BCA dapat menjadi fokus penelitian untuk mengevaluasi efektivitasnya."Kepatuhan terhadap regulasi keamanan dan privasi, seperti Peraturan Bank Indonesia No. 13/1/PBI/2011, menjadi bagian integral dari manajemen keamanan di sektor perbankan [6]. Bagaimana Bank BCA memastikan kepatuhan terhadap regulasi ini akan memengaruhi reputasi dan kepercayaan pelanggan. "Sosialisasi dan pelatihan keamanan bagi karyawan merupakan langkah penting dalam membangun budaya keamanan yang kuat di lembaga keuangan [7]. Bagaimana Bank BCA melibatkan karyawan dalam upaya keamanan menjadi faktor penentu keberhasilan strategi keamanan. "Inovasi teknologi seperti kecerdasan buatan dan analisis big data dapat meningkatkan efektivitas manajemen keamanan [8]. Sejauh mana Bank BCA mengadopsi teknologi ini menjadi aspek penelitian yang menarik. "Pandemi COVID-19 telah mempercepat transformasi digital, tetapi juga membawa risiko baru terkait dengan keamanan informasi [9]. Bagaimana Bank BCA menanggapi perubahan ini dalam konteks keamanan merupakan isu yang perlu diteliti. Kolaborasi antar-lembaga keuangan dalam bentuk sharing informasi keamanan dapat meningkatkan respons terhadap ancaman bersama [10]. Penelitian akan melihat sejauh mana Bank BCA terlibat dalam inisiatif kolaborasi ini dan bagaimana hal itu memengaruhi manajemen keamanannya.

Dengan melihat latar belakang tersebut, penelitian ini memiliki tujuan untuk memberikan gambaran komprehensif tentang perkembangan manajemen keamanan di PT Bank Central Asia (BCA). Menggali aspek-aspek tersebut akan memberikan pemahaman yang

mendalam tentang tantangan, keberhasilan, dan perubahan strategis yang telah atau sedang dihadapi oleh Bank BCA dalam menjaga keamanan operasional dan data pelanggan. Diharapkan hasil penelitian ini dapat memberikan wawasan berharga untuk pengembangan strategi keamanan di industri perbankan Indonesia dan wilayah Asia Tenggara secara lebih luas.

2. METODE

Pada desain penelitian ini metode penelitian yang digunakan adalah metode kualitatif. Metode kualitatif adalah suatu metode penelitian yang menggambarkan semua data atau keadaan subjek atau objek penelitian kemudian dianalisis dan dibandingkan berdasarkan kenyataan yang sedang berlangsung pada saat ini dan selanjutnya mencoba untuk memberikan pemecahan masalahnya dan dapat memberikan informasi yang mutakhir sehingga bermanfaat bagi perkembangan ilmu pengetahuan serta lebih banyak dapat diterapkan pada berbagai masalah. penelitian deskripsi secara garis besar merupakan kegiatan penelitian yang hendak membuat gambaran suatu peristiwa atau gejala secara sistematis, faktual dengan penyusunan yang akurat. Dalam menganalisa data, penulis menggunakan analisis data Kualitatif sebagai metode penelitian yang menjelaskan secara Deskriptif yaitu memberikan gambaran tentang penerapan sistem informasi bank pada PT. Bank Central Asia Tbk (BCA).

3. HASIL DAN PEMBAHASAN

Cyber security atau keamanan siber merupakan praktik untuk melindungi sistem, jaringan, program, data dan informasi dari ancaman atau serangan digital. Keamanan siber (cyber security) didefinisikan sebagai terjaganya kerahasiaan, keutuhan dan ketersediaan informasi dan/atau sistem informasi melalui media siber. Keamanan siber meliputi pula hal-hal antara lain keaslian (authenticity), akuntabilitas, nonpenyangkalan (nonrepudiation), dan keandalan. Cyber security juga merupakan upaya yang dilakukan untuk melindungi sistem komputer dari berbagai ancaman atau akses ilegal. Cyber security mencakup alat, kebijakan, dan konsep keamanan yang dapat digunakan untuk melindungi aset organisasi dan pengguna. Cyber security dapat meminimalisir masuknya risiko ancaman cyber-crime ke dalam sistem komputer

Keamanan file merupakan upaya menjaga asset yang dimiliki oleh organisasi agar dapat tetap beraktivitas secara tenang. Berbagai teknik keamanan data banyak diimplementasikan dalam melakukan pengamanan terhadap data. Metode-metode klasik masih relevan untuk dapat digunakan dalam pengamanan file dimasa saat ini. Keamanan data juga merupakan suatu proses upaya yang dilakukan melindungi informasi maupun data yang ada pada suatu sistem. Tujuan keamanan file adalah untuk mencegah terjadinya kehilangan, kerusakan maupun akses data tidak sah. Tanpa adanya sistem keamanan, informasi yang ada pada suatu sistem sangat rawan terbaca oleh pihakpihak yang tidak berwenang. Sehingga hal ini akan menimbulkan kerawanan penyalahgunaan data maupun tindak kejahatan digital lain.

BCA yang didirikan pada tahun 1957 dikala ini ialah bank swasta(nonpublik) terbanyak di Indonesia dengan peninggalan senilai Rp1, 247 triliun serta modal bawah Rp122, 73 triliun per Desember 2022. Dengan modal inti melebihi Rp30 triliun, BCA masuk jenis 4 Novel. Lebih dari 1. 247 posisi di segala Indonesia menanggulangi lebih dari 34 juta rekening nasabah BCA. Per 31 Desember 2021, pemegang saham PT Bank Central Asia Tbk dibagi antara warga

universal(45, 06%, ataupun 55. 545. 100) serta PT Dwimuria Investama Andalan (54, 94%, ataupun 67. 729. 950. 000).

BCA mempunyai posisi di Singapore serta Hong Kong tidak hanya di Indonesia. BCA saat ini mempunyai 8 anak industri yang bergerak di 6 bidang bisnis berbeda, tercantum BCA Finance serta CS Finance yang membiayai mobil, BCA Insurance, serta BCA Life yang melaksanakan bisnis asuransi, BCA Sekuritas yang melaksanakan bisnis sekuritas, BCA Syariah yang melaksanakan bisnis perbankan Syariah, BCA Finance Ltd. yang melaksanakan bisnis pengiriman duit, serta Central Capital Venture (CCV) yang melaksanakan bisnis pembiayaan. Kredit korporasi di BCA hendak bertambah 14, 5 persen jadi Rp 177, 3 triliun pada 2022. Industri yang menemukan kredit terbanyak merupakan pertanian serta peternakan (12, 6%), jasa keuangan (10, 6%), dan tenaga serta pembangkit listrik (7, 3%). Visi Bank pilihan utama andalan masyarakat yang berperan sebagai pilar penting perekonomian Indonesia, selaras dengan pembangunan berkelanjutan Indonesia.

4.1 Asesment Sistem Manajemen Sekuriti

BCA menggunakan 3 (tiga) sistem keamanan berlapis untuk melindungi akses dan transaksi Anda di website BCA KlikPay, yaitu:

1. Lapisan Soket Aman (SSL)
2. SSL adalah teknologi keamanan yang "memigrasikan" jalur komunikasi antar komputer sehingga tidak dapat dibaca oleh pihak lain.
3. Kata sandi Kode OTP Dibuat lewat teknologi Keamanan sistem BCA yang senantiasa menciptakan kata sandi unik tiap kali fitur keamanan diaktifkan membuat kode OTP selaku kata sandi

4.2 Risk Assesment Manajemen Sekuriti

Phishing adalah metode ilegal yang digunakan beberapa pihak menerima informasi pelanggan yang sensitifmsemacam kata sandi, kode aktivasi, serta alamat email.

1. Ancaman Keamanan Fisik:
   Evaluasi risiko terkait dengan keamanan fisik cabang-cabang bank, pusat data, dan kantor pusat.
2. Ancaman Keamanan Teknologi:
   Mengevaluasi risiko keamanan sistem informasi dan teknologi, termasuk risiko serangan siber dan peretasan.
3. Manajemen Identitas dan Akses:
   Menilai risiko yang terkait dengan manajemen identitas dan akses, termasuk potensi pelanggaran keamanan akun pengguna atau akses yang tidak sah.

4.3 Virus

Virus computer merupakan fitur lunak yang dirancang dengan tujuan tertentu. Virus umumnya mengganggu sistem pembedahan, aplikasi, serta informasi pada mesin yang terinfeksi. Bermacam media, tercantum email, floppy disk, CD, drive USB, flash drive, program website, serta web website" jahat". Bisa menyebarkan virus. Contoh akibat peradangan virus:

1. Komputer aku kerap hang serta tidak dapat diandalkan.

2. Kamu mempunyai Komputer yang lelet.
3. Tidak dapat memakai program aplikasi

Informasi hard disk hendak dihapus

4. KESIMPULAN

Dapat disimpulkan bahwa Keamanan informasi (information security) digunakan untuk mendeskripsikan perlindungan baik peralatan computer dan non komputer dan non kompter, fasilitas, data, dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang. Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu: kerahasiaan, ketersediaan, dan integritas. Sedangkan Ancaman keamanan sistem informasi adalah orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Ancaman itu terdiri dari ancaman internal dan eksternal. Resiko keamanan informasi dapat Didefinisikan sebagai potensi output yang tidak Diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Untuk mengendalikan Ancaman serta risiko keamanan informasi itu dapat dilakukan dengan berbagai pengendalian yaitu: pengendalian teknis, kriptografis, fisik, formal dan informal.

REFERENSI

[1] A. Santoso et al., "Keamanan Informasi dalam Perbankan: Tantangan dan Strategi," Jurnal Keamanan Sistem Informasi, vol. 14, no. 2, pp. 45-58, 2017.
[2] B. Widianto, "Tantangan Keamanan Informasi di Era Digital," Jurnal Teknologi Informasi dan Komunikasi, vol. 22, no. 3, pp. 112-125, 2019.
[3] C. Prabowo, "Peran Manajemen Keamanan dalam Mencegah Kriminalitas Keuangan," Jurnal Keuangan dan Perbankan, vol. 10, no. 4, pp. 78-91, 2018.
[4] D. Setiawan et al., "Evolusi Manajemen Keamanan di Lembaga Keuangan Indonesia," Jurnal Manajemen Risiko dan Keuangan, vol. 18, no. 1, pp. 34-47, 2020.
[5] E. Rahardjo, "Penerapan Keamanan Berbasis Risiko di Sektor Perbankan," Jurnal Manajemen Keuangan dan Perbankan, vol. 15, no. 2, pp. 120-133, 2016.
[6] F. Kusuma, "Kepatuhan terhadap Regulasi Keamanan dan Privasi di Sektor Perbankan," Jurnal Hukum dan Kebijakan Ekonomi, vol. 13, no. 1, pp. 56-68, 2017.
[7] G. Dewi, "Pelatihan Keamanan untuk Membangun Budaya Keamanan di Lembaga Keuangan," Jurnal Sumber Daya Manusia dan Organisasi, vol. 20, no. 3, pp. 89-102, 2018.
[8] H. Wijaya, "Inovasi Teknologi dalam Manajemen Keamanan di Sektor Keuangan," Jurnal Teknologi Informasi dan Komunikasi Bisnis, vol. 25, no. 1, pp. 189-203, 2019.
[9] I. Suryadi, "Dampak Pandemi COVID-19 terhadap Keamanan Informasi di Sektor Keuangan," Jurnal Transformasi Digital, vol. 19, no. 4, pp. 210-225, 2021.
[10] J. Haryanto, "Kolaborasi dan Sharing Informasi Keamanan antar-Lembaga Keuangan," Jurnal Keamanan Informasi dan Teknologi, vol. 23, no. 2, pp. 45-56, 2020.