

**PERKEMBANGAN MANAGEMENT SEKURITI DI PT BANK
CENTRAL ASIA (BCA)**

Ahmad Sofiyah¹, Ulfa Amelia², Khoiridha Askiyyah³, Fried Sinlae⁴

E-mail: 202110715229@mhs.ubharajaya.ac.id¹, 202110715110@mhs.ubharajaya.ac.id²,
202110715164@mhs.ubharajaya.ac.id³, fried.sinlae@dsn.ubharajaya.ac.id⁴

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.

Kata Kunci: *Manajemen Keamanan, Teknologi Keamanan, Keamanan Fisik*

PENDAHULUAN

Keamanan informasi dan manajemen sekuriti menjadi aspek yang semakin krusial dalam konteks globalisasi dan pertumbuhan teknologi informasi di abad ke-21. Di Indonesia, seperti halnya di banyak negara lainnya, perkembangan manajemen sekuriti mengalami dinamika yang signifikan seiring dengan transformasi digital yang pesat. Perubahan-perubahan tersebut menciptakan tantangan baru sekaligus peluang dalam upaya menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam suatu organisasi. Pentingnya manajemen sekuriti di Indonesia juga tercermin dalam upaya pemerintah untuk menciptakan lingkungan yang aman dan andal dalam pemanfaatan teknologi informasi. Melalui inisiatif-inisiatif seperti pembentukan kebijakan, regulasi, dan pendidikan, pemerintah berupaya untuk meningkatkan kapasitas organisasi dalam mengelola dan melindungi informasi mereka.

Pembahasan tentang manajemen sekuriti fisik di dalam perusahaan yang diambil ialah di PT Bank Central Asia Tbk (disingkat BCA) (IDX: BBCA) adalah bank swasta terbesar di Indonesia. Bank ini didirikan pada 21 Februari 1957 dan pernah menjadi bagian penting dari Grup Salim. Bank tersebut kini dimiliki oleh Djarum, salah satu grup manufaktur rokok terbesar keempat di Indonesia.

Dalam menjamin pengamanan di PT. BCA Tbk diperlukan manajemen sekuriti dengan memanfaatkan penggunaan sumber daya secara efektif untuk mencapai sasaran, dan dapat diartikan sebagai pimpinan yang bertanggung jawab atas jalannya perusahaan dan organisasi.

METODE PENELITIAN

Pada desain penelitian ini metode penelitian yang digunakan adalah metode kualitatif. Menurut Moleong (2017:6) 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).

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.

Misi

Strategi keberlanjutan untuk mendukung implementasi Keuangan Berkelanjutan dilakukan melalui:

- Penyediaan pembiayaan kegiatan usaha,berkelanjutan;
- Pengembangan kapasitas intern; dan
- Penyesuaian organisasi, manajemen risiko, tata kelola, dan/atau standar prosedur operasional

A. 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.

Karena susah buat sediakan layanan perbankan online yang memikirkan keamanan tiap browser sebab banyaknya alterasi browser Internet. Dikala ini, cuma BCA menawarkan layanan perbankan online yang paling sesuai untuk digunakan dengan Microsoft Internet Explorer 8 ke atas. BCA menyampaikan permohonan maaf atas ketidaknyamanan tersebut. yang ditimbulkan

B. Risk Assesment Manajemen Sekuriti

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

1. Membuat web website palsu yang mempunyai URL serta desain yang mirip dengan web website merchant BCA KlikPay ataupun BCA KlikPay yang legal.
2. Mengirimi Kamu email ataupun pesan dengan tautan URL ataupun login yang memohon alamat email, kata sandi, kode aktivasi, serta OTP Kamu buat masuk. kata sandi, kode aktivasi, dan OTP.
3. Berpura- pura jadi karyawan BCA serta memohon data dari Kamu
4. Jika Kirim email ke halobca@bca. co. id ataupun telepon Halo BCA bila Kamu memperoleh email, telepon, ataupun pesan yang Kamu yakini berasal dari BCA (1500888) di handphone Anda. Jika Anda telah memberikan informasi yang diperlukan atau Anda yakin ada orang lain yang mengetahui akun dan password BCA KlikPay Anda, segera hubungi Halo BCA 1500888 di ponsel Anda.

C. Virus

Virus computer merupakan fitur lunak yang dirancang dengan tujuan tertentu. Virus umumnya mengganggu sistem pembedahan, aplikasi, serta informasi pada mesin yang terinfeksi. Berbagai 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
4. Informasi hard disk hendak dihapus.

Seperti halnya Worm dimaksudkan buat menyebar dengan kilat di antara komputer yang berbeda, semacam halnya virus. Walaupun worm umumnya memunculkan lebih sedikit kehancuran daripada virus, mereka bisa digunakan buat mengangkat bermacam berbagai muatan serta lampiran, tercantum yang bermusuhan

KESIMPULAN

Dapat disimpulkan bahwa Keamanan informasi (information security) digunakan untuk mendeskripsikan perlindungan baik peralatan computer dan non komputer dan non komputer, 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.

DAFTAR PUSTAKA

- E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.
- P. E. Widjaya and Y. Sugiarti, "Penerapan Risk Management Untuk Meningkatkan Non-Financial Firm Performance Di Perusahaan Murni Jaya," *J. Ilm. Mhs. Univ. Surabaya*, vol. 2, no. 1, pp. 1–18, 2013, [Online]. Available: <https://media.neliti.com/media/publications/185290-ID-none.pdf>
- A. Samsudin et al., "Pengaruh Kualitas Pelayanan terhadap Keputusan Konsumen Dalam Menggunakan Jasa pada PT BCA," *El-Mujtama J. Pengabd. Masy.*, vol. 3, no. 2, pp. 531–538, 2023, doi: 10.47467/elmujtama.v3i2.2777.
- E. Soesanto, N. A. Ningsih, M. I. Faturrahman, and L. Khoerunisa, "Peranan Sistem Pengamanan File Dan Cyber Security Terhadap Obyek Vital Pada PT Bank Central Asia (BCA)," *J. Akuntan Publik*, vol. 1, no. 2, pp. 210–216, 2023.
- E. Soesanto, F. Saputra Program Studi Manajemen, U. Bhayangkara Jakarta Raya Dita Puspitasari Program Studi Manajemen, and U. Bhayangkara Jakarta Raya Bayu Putra Danaya, "Analisis Sistem Manajemen Sekuriti: K3 dan Beban Kerja di PT. XYZ," *J. Ris. dan Inov. Manaj.*, vol. 1, no. 2, pp. 139–150, 2023, [Online]. Available: <https://doi.org/10.59581/jrim-widyakarya.v1i2.393>
- T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware