Jurnal Akuntan Publik
Vol. 1, No. 2 Juni 2023
e-ISSN: 2775-4200; p-ISSN: 2580-8028, Hal 210-216
DOI: https://doi.org/10.59581/jap-widyakarya.v1i2.454

Peranan Sistem Pengamanan File Dan Cyber Security Terhadap Obyek Vital Pada PT Bank Central Asia (BCA)

Edy Soesanto
Fakultas Ekonomi Bisnis, Universitas Bhayangkara Jakarta Raya

Nova Astia Ningsih
Fakultas Ekonomi Bisnis, Universitas Bhayangkara Jakarta Raya

Muhammad Ilham Faturrahman
Fakultas Ekonomi Bisnis, Universitas Bhayangkara Jakarta Raya

Lili Khoerunisa
Fakultas Ekonomi Bisnis, Universitas Bhayangkara Jakarta Raya

Alamat : Jl. Harsono RM No.67, RT.2/RW.4, Ragunan, Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550
novaastia123@gmail.com

Abstract : *Along with the rapid development of information technology, customer interaction with BCA digitally has also increased. This is followed by the risk of technology crime, so BCA continues to improve its information technology security system. The development of BCA's data security system is carried out with the aim of protecting data security and ensuring information technology systems are always ready to serve customer transactions, including preventing and anticipating cybercrimes and potential fraud. National vital objects have an important role in the life of the nation and state, both in terms of economic, political, social, cultural, defense, and security aspects. National vital objects also have a quite strategic role in national development. Data Loss Prevention (DLP) is a data security strategy implemented by BCA on an ongoing basis to increase the security of important electronic information from information theft or access by unauthorized parties. To ensure security in accessing BCA's internal applications that are connected to the internet, BCA applies additional security in the form of two-factor authentication to ensure access to the application is carried out by the right person. BCA has also used a data classification solution to ensure that every piece of data in the company is classified according to the level of data confidentiality.*

Keywords: *Information Technology, Security Systems, Cyber-crime, National Vital Objects. Data Security.*

Abstrak : seiring dengan pesatnya teknologi informasi, interaksi nasabah dengan BCA secara digital juga meningkat. Hal ini diikuti oleh risiko kejahatan teknologi, sehingga BCA terus meningkatkan sistem keamanan Teknologi Informasi. Pengembangan sistem keamanan data BCA dilakukan dengan tujuan untuk melindungi keamanan data dan memastikan sistem Teknologi Informasi dapat selalu siap melayani transaksi nasabah, termasuk menangkal dan mengantisipasi *cyber-crime* serta potensi fraud. Obyek vital nasional memiliki peran penting bagi kehidupan bangsa dan negara baik ditinjau dari aspek ekonomi, politik, sosial, budaya, pertahanan dan keamanan, obyek vital nasional juga mempunyai peran yang cukup strategis dalam pembangunan nasional. *Data Loss Prevention* (DLP) merupakan strategi pengamanan data

Received April 27, 2023; Revised Mei 12, 2023; Accepted Juni 04, 2023
* Edy Soesanto, novaastia123@gmail.com

yang dilakukan BCA secara berkelanjutan untuk meningkatkan pengamanan informasi elektronik penting dari pencurian informasi maupun akses oleh pihak yang tidak berkepentingan. Guna memastikan keamanan dalam mengakses aplikasi internal BCA yang terkoneksi dengan internet, BCA menerapkan pengamanan tambahan berupa *two factor authentication* untuk memastikan akses aplikasi tersebut dilakukan oleh orang yang tepat. BCA juga telah menggunakan solusi klasifikasi data untuk memastikan setiap data yang ada di dalam perusahaan diklasifikasi sesuai dengan tingkat kerahasiaan datanya.

Kata kunci: Teknologi Informasi, Sistem Keamanan, *Cyber-crime,* Objek Vital Nasional, Keamanan Data

PENDAHULUAN

BCA merupakan salah satu bank swasta yang pertama kali menerima sertifikasi bergengsi yaitu Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 untuk seluruh entitas yang mengelola transaksi dan data pemegang kartu, termasuk data center. Selain itu, BCA juga memperoleh sertifikasi ISO 20000-1:2018 dalam rangka meningkatkan sistem manajemen layanan atau Service Management System (SMS).

BCA telah memiliki sertifikasi ISO 27001 terkait standar sistem manajemen keamanan informasi pada sistem jaringan dan data center. Selain itu BCA termasuk salah satu bank swasta yang pertama kali menerima sertifikasi bergengsi yaitu PCI DSS 3.2.1 untuk seluruh entitas yang mengelola transaksi dan data pemegang kartu, termasuk data center.

Adapun tujuan dari peneilitan ini yaitu Untuk mengetahui bagaimana pengaruh cyber security terhadap objek vital nasional PT Bank Central Asia (BCA). Untuk memastikan memberikan keamanan layanan bagi setiap nasabah, direktur teknologi informasi turut mengawasi melalui laporan yang disampaikan oleh divisi strategic it group secara berkala. BCA memberikan pelatihan terkait *e-learning social engineering awareness* bagi seluruh pekerja BCA. Selain itu BCA juga tidak menghadapi kasus signifikan terkait pelanggaran maupun penyalahgunaan data dan privasi nasabah. Selama tahun 2020, tidak ada data nasabah yang hilang. Maka, tidak ada sanksi/denda yang dikenakan kepada BCA maupun pekerjanya.

TINJAUAN PUSTAKA

1. Objek Vital Nasional

Obyek vital nasional memiliki peran penting bagi kehidupan bangsa dan negara baik ditinjau dari aspek ekonomi, politik, sosial, budaya, pertahanan dan keamanan, obyek vital nasional juga mempunyai peran yang cukup strategis dalam pembangunan nasional (Keppres No. 63 Thn 2004). Di lain pihak, dimensi ancaman dan gangguan keamanan semakin berkembang dengan beragam risiko dan dampaknya. Ancaman dan gangguan keamanan terhadap obyek vital nasional secara langsung maupun tidak langsung berdampak pada sistem perekonomian nasional, stabilitas politik, serta keamanan nasional.

2. Keamanan File

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 pihak-pihak yang tidak berwenang. Sehingga hal ini akan menimbulkan kerawanan penyalahgunaan data maupun tindak kejahatan digital lain.

3. Cyber *Security*

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 (*non-repudiation*), 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.

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 PENELITIAN DAN PEMBAHASAN

Bank Cental Asia baru serius menggunakan teknologi informasi sekitar tahun 1989 dengan tujuan untuk membedakan pelayanan dengan bank lain. Untuk itu Bank Cental Asia harus menginvestasikan dana yang besar untuk membangun sistem informasinya. Dengan menggunakan VSAT, BCA mampu menghubungkan antar cabangnya secara *on line*. Produk BCA yang selama ini memanfaatkan teknologi informasi meliputi telegraphic tansfer, mail transfer, ATM dan phone banking. Sampai tahun 1995 jumlah ATM BCA mencapai 500 unit. Hal ini berkat kemudahan yang selama ini ditawarkan BCA.

Sistem informasi BCA juga dimanfaatkan untuk meningkatkan efisiensi dan produktivitas cabang. Penjurnalan pembukuan sekarang dilakukan secara otomatis, begitu juga pemindahan antar rekening. Dengan demikian pekerjaan para auditor menjadi lebih ringan. Kehadiran Local Area Network (LAN) digunakan untuk pendistribusian data entry dan pemrosesan transaksi. Pada hari-hari sibuk tak kurang dari 1 juta transaksi harus diproses. Sedangkan fasilitas e-mail digunakan untuk mempermudah komunikasi antar cabang. Pada masa sekarang agar suatu perusahaan tetap mampu survive di tengah jaman yang terus menerus berubah secara cepat seperti sekarang ini, salah satu kata kuncinya menurut Thurow (1997) adalah adaptif. Hal ini disebabkan perubahan jaman akan membawa pula perubahan pada sifat masyarakat dan tentu saja pada sifat dunia ekonomi secara khusus. Agar perusahaan mampu selalu adaptif terhadap perubahan yang muncul, maka perusahaan harus mempersiapkan diri terhadap berbagai kemungkinan yang dapat terjadi. Untuk itu perusahaan harus mempunyai berbagai data dan informasi tentang segala sesuatu yang ada di sekitar perusahaan. Dengan data-data yang ada tersebut, perusahaan dapat membuat berbagai macam alternatif skenario strategi. Selanjutnya

dengan pengolahan informasi yang terus menerus dari data yang masuk dari hari ke hari, perusahaan dapat melakukan analisis atas alternatif-alternatif skenarionya, untuk mencapai skenario terbaik bagi pelaksanaan kegiatan di waktu-waktu mendatang, demikian seterusnya. Hal seperti ini tentu saja memerlukan dukungan suatu sistem informasi yang baik. Pengguna internet di Indonesia dan di seluruh dunia dalam satu dasawarsa terakhir, mengalami perkembangan sangat pesat. Bahkan kini, internet telah menjadi sarana bisnis dan digunakan lebih dari 1,5 miliar orang di dunia. Pesatnya jumlah pengguna internet, memacu PT. Bank Central Asia.Tbk (BCA) meluncurkan *E-Commerce* BCA, yakni sebuah layanan pemrosesan transaksi online kartu kredit di website merchant BCA. Layanan *E-Commerce* BCA dirancang untuk memenuhi kebutuhan para merchant dalam meningkatkan penjualan dan menggarap potensial market yang lebih luas. Melalui layanan *E-Commerce* BCA, para merchant dapat memiliki online payment processing menu pada website mereka serta dilengkapi layanan penyelesaian transaksi *settlement*. Untuk memberikan layanan *E- Commerce* ini, BCA didukung *MasterCard internet Gateway Service* (MiGS) sebagai payment gateway yang memberikan solusi pembayaran komprehensif. Pembayaran yang dilakukan oleh pelanggan di website merchant dengan menggunakan kartu kredit MasterCard ataupun Visa, dapat diproses melalui fasilitas E-Commerce BCA.

E-Commerce BCA terlihat dari item pelayanan yang terdapat pada I-Banking bank BCA terdapat 10 Service yang bisa digunakan oleh nasabahnya, yaitu: Pembelian, Pembayaran, Transfer Dana, Informasi Rekening, Informasi Kartu Kredit, Informasi Lainnya, Status Transaksi, Historis Transaksi, Administrasi, dan E-mail.

Prioritas utama BCA adalah memastikan keamanan aplikasi *e-channel* BCA untuk meningkatkan kepercayaan dan kenyamanan nasabah dalam bertransaksi. BCA meningkatkan keamanan pada platform-platform transaksi di kanal digital dengan cara memanfaatkan teknologi machine learning dan artificial intelligence untuk melakukan deteksi awal adanya malware pada komputer nasabah. Secara berkala, BCA melakukan pengujian kerentanan aplikasi bekerja sama dengan konsultan keamanan TI. Di sisi pengamanan *mobile device*, BCA telah menerapkan Secure E-mail pada mobile device guna mengamankan e-mail yang tersimpan di mobile device, dan juga Anti Virus untuk memastikan mobile device bebas dari *malware*. Selain itu, untuk pengamanan e-mail juga dilakukan penambahan kemampuan e-mail sandboxing untuk memastikan e-mail yang masuk ke BCA bebas dari *malware*, serta penambahan e-mail tagging untuk memberikan informasi tambahan apabila e-mail berasal dari luar BCA.

BCA juga telah menerapkan solusi perlindungan container untuk memastikan keamanan platform serta aplikasinya. Di sisi jaringan sebagai jalur lalu lintas transaksi perbankan, BCA juga selalu meningkatkan keamanannya antara lain dengan mulai mengimplementasikan *Next-Generation Intrusion Prevention System* dengan kemampuan deteksi dan proteksi terhadap *vulnerability exploit* dan *malware* yang lebih mutakhir sehingga meningkatkan keamanan jaringan Bank.

KESIMPULAN DAN SARAN

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.

Saran

Saat ini, perusahaan dapat melakukan pengawasan serta pengelolaan yang tepat bagi *privileged access* untuk melindungi sistem informasi objek vital nasional perusahaan, yaitu melakukan 5 cara berikut ini dengan solusi Privileged Access Management. Berikut adalah 5 cara yang dapat dilakukan khususnya oleh perusahaan Bank Central Asia (BCA):

1. Mencegah pencurian kredensial yang berasal dari serangan eksternal
2. Mencegah aktivitas tertentu pada sistem
3. Mencegah eksalasi dan penyalahgunaan hak akses istimewa yang berasal dari pihak internal
4. Memenuhi kebutuhan audit dan compliance
5. menempatkan kontrol keamanan yang efektif untuk akses yang diperlukan oleh pihak ketiga

DAFTAR PUSTAKA

Bank Central Asia. (2010, January). Info BCA. hal. 16-18.

Bank Central Asia. (2015). Annual Report. Jakarta: Bank Central Asia Tbk.

(2017, November). Keamanan Informasi. Dikutip 17 November 2019 dari MMSI Binus: https://mmsi.binus.ac.id/2017/11/17/keamanan-informasi/

Suheri, Agus, (2010) Pengamanan File Dengan Kompresi Huffman dan Penyamaran Data Steganografi, Media Jurnal Informatika, Vol.2, Jurusan Teknik Informatika, Universitas Suryakancana, Cianjur

Ariyus, Dony,(2006) Computer Security, Andi Offset, Jogja

Putra, Y. M., (2018). Keamanan Informasi. Modul Kuliah Sistem Informasi Manajemen. Jakarta: FEB-Universitas Mercu Buana

KEPUTUSAN PRESIDEN REPUBLIK INDONESIA NOMOR 63 TAHUN 2004 TENTANG PENGAMANAN OBYEK VITAL NASIONAL:

https://jdih.esdm.go.id/peraturan/Keppres%20No.%2063%20Thn%202004.pdf