Student Research Journal
Vol.1, No.3 Juni 2023
e-ISSN: 2964-3252; p-ISSN: 2964-3260, Hal 227-238
DOI: https://doi.org/10.55606/srjyappi.v1i3.334

Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA)

Edy Soesanto
Dosen Fakultas Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya

Nova Astia Ningsih
Mahasiswa Fakultas Ekonomi & Bisnis, Universitas Bhayangkara Jakarta Raya

Lili Khoerunisa
Mahasiswa Fakultas Ekonomi & Bisnis, Universitas Bhayangkara Jakarta Raya

Muhammad Ilham Faturrahman
Mahasiswa 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
Email: edy.soesanto@dsn.ubharajaya.ac.id, novaastia123@gmail.com, novaastia123@gmail.com, ifaturrahman38@gmail.com

Abstract : *In this era of very rapid growth of information systems, the security of information is something that must be considered, because if information can be accessed by unauthorized or irresponsible people, then the accuracy of the information will be doubted, it will even become information that is healed. Basically a secure system will protect the data in it such as user assistance (user identification), user authentication (user authentication), user authorization (user authorization). Several possible attacks (Hacking) that can be carried out, such as Intrusion, denial of services, joyrider, vandals, piracy, sniffing, spoofing and others. There are many kinds of threats to information systems, including: data theft, illegal use of systems, illegal data destruction, illegal data modification, system failures, human error (HR-human resources), natural disasters. The purpose of information security is prevent threats to the system and detect and repair damage that occurs to the system.*

Keywords: *Historical security, security protection, security anticipation, security assessment, risk assessment.*

Abstrak : Di era sistem informasi yang berkembang dengan sangat cepat keamanan informasi harus diperhatikan, karena jika informasi tersebut berada di tangan orang yang tidak berwenang atau tidak bertanggung jawab, keakuratan informasi tersebut dipertanyakan dan justru akan menjadi informasi yang menyesatkan. Pada dasarnya, sistem yang aman melindungi informasi yang dikandungnya dengan cara yang sama seperti mengidentifikasi pengguna (identifikasi pengguna), memverifikasi keaslian pengguna (autentikasi pengguna), dan memberikan izin pengguna (otorisasi pengguna). Beberapa kemungkinan serangan (peretasan) dimungkinkan, seperti Gangguan (intrusion), penolakan layanan (denial of services), joyriders, vandalisme, pembajakan, pengintaian, peniruan identitas dan lain-lain. Ada banyak peringatan tentang sistem informasi, termasuk: Tujuan keamanan data adalah untuk mencegah ancaman terhadap sistem dan untuk mendeteksi serta memperbaiki kerusakan pada sistem.

Kata Kunci: Historis sekuriti, protek sekuriti, antisipasi sekuriti, asesmen sekuriti, risk asesmen.

Received April 25, 2023; Revised Mei 12, 2023; Accepted Juni 05, 2023
** Edy Soesanto, edy.soesanto@dsn.ubharajaya.ac.id*

PENDAHULUAN

1. Latar Belakang

Bank adalah salah satu jalur kehidupan dalam perekonomian sebuah Negara, jika tidak ada bank bisa dibayangkan bagaimana sulitnya menerima dan juga mengirimkan uang. Menurut UU Perbankan No. 10 Tahun 1998, bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan meminjamkannya kepada masyarakat dalam bentuk kredit dan bentuk lainnya untuk meningkatkan taraf hidup masyarakat. Dapat dilihat bahwa perbankan melakukan tiga kegiatan yaitu menghimpun dana masyarakat dalam bentuk simpanan (kiriman uang, tabungan dan deposito), menyalurkan dana dalam bentuk kredit dan memberikan jasa perbankan lainnya.

Fokusnya tidak hanya pada masalah kuantitatif seperti pendapatan bunga bank, tetapi juga pada aspek kualitatif, baik dari sisi produk perbankan yang ditawarkan, layanan yang ditawarkan, kepercayaan dan citra bank yang baik, yang pada akhirnya memiliki dampak yang signifikan. pada loyalitas pelanggan. Pada tahap perkembangan saat ini, bank mulai menyadari pentingnya kondisi yang mempengaruhi nasabah. Tingkat layanan merupakan faktor dominan dalam layanan perbankan. Sebagai contoh, nasabah yang merasa pelayanannya berkualitas tinggi juga merasa sangat puas dan percaya dengan efisiensi bank yang ada. Jika bank memiliki citra yang baik maka nasabah juga akan merasa nyaman dan akan tercipta tingkat loyalitas yang tinggi. Dengan cara ini, nasabah biasanya merupakan nasabah setia bank.

Bank BCA merupakan salah satu perusahaan yang bergerak di industri jasa, bank didorong untuk melayani nasabahnya dengan baik. Studi ini dilakukan pada tahun 2014 oleh Majalah Service Excellence (anggota Grup Majalah Marketing) (www.infobanknews.com). Menegaskan bahwa Bank BCA kembali meraih juara pertama yaitu Service Quality Award 2014. Evaluasi didasarkan pada tiga dimensi utama: Perceived Service Best (PSB) adalah reaksi pelanggan terhadap keberadaan merek layanan lain dengan layanan yang lebih baik, Perceived Service Value (PSV) adalah reaksi pelanggan terhadap perbandingan harga. Layanan berbayar dan diterima, Perceived Service Quality (PSQ) adalah respons pelanggan terhadap layanan yang diterima olehnya, yang memengaruhi aksesibilitas layanan (kemudahan penggunaan saat menggunakan layanan) dan proses layanan (kesederhanaan, kecepatan, ketepatan, dan kenyamanan). layanan meliputi proses, resolusi layanan (kecepatan dan kelengkapan penanganan

keluhan), dan orang (kemampuan hard skill dan juga soft skill petugas frontline termasuk grooming serta appearance).

Nasabah secara langsung atau tidak langsung menyampaikan evaluasi terhadap layanan yang telah dibelinya. Dua faktor utama yang menjadi pedoman pelanggan yaitu pelayanan yang diterima dan pelayanan yang diharapkan oleh pelanggan (Tatik Suryani, 2013:89). Di perusahaan jasa, kualitas jasa sering diusulkan sebagai kesetaraan yang jelas antara kinerja yang diharapkan dan kinerja yang diterima. Mempromosikan layanan pelanggan yang baik dan menarik pelanggan untuk bersaing dan mengurangi pangsa pasar mereka juga mempengaruhi citra perusahaan perbankan di mata pelanggan.

Bank khususnya Bank BCA menekankan bahwa peningkatan kualitas pelayanan yang baik mempengaruhi citra perusahaan perbankan di mata nasabah. Citra perusahaan memiliki pengaruh yang signifikan terhadap pengambilan keputusan pelanggan (Tatik Suryani, 2013:85). Menciptakan citra yang baik dengan pelanggan berkontribusi pada citra positif perusahaan.

Selain itu, kepercayaan juga sangat penting bagi Nasabah. Nasabah mengkhawatirkan keamanan dana mereka (takut dana mereka tiba-tiba hilang). Bank BCA menerapkan berbagai cara untuk menjaga kepercayaan nasabah dan memastikan keamanan dana nasabah. Caranya dengan berinteraksi dengan komunitas, merayakan BCA, dan menyambut BCA.

Orang-orang peduli dengan layanan bank. Masyarakat sekarang mengeluh, malah orang berani menyebarkan keluhan itu di media. Hal ini tercermin dari banyaknya pengaduan di media, serta keberatan langsung terhadap bank atas pelayanan yang dianggap kurang memuaskan. Karena itu, layanan diperlukannya Kepuasan nasabah harus datang dari bank agar nasabah terkesan, kepercayaan nasabah meningkat dan citra bank di mata nasabah meningkat.

2. Rumusan Masalah

a. Bagaimana risiko keamanaan informasi data dalam penggunan teknologi terhadap PT. Bank central Asia (BCA) ?
b. Bagaimana pengaplikasian sistem informasi data untuk menjaga keamanan PT. Bank Central Asia (BCA) ?

3. Tujuan penelitian

a. Untuk dapat Mengetahui Penjelasan Mengenai Keamanan Informasi Data Bank BCA
b. Untuk dapat Mengetahui Tujuan Keamanan Informasi Data Bank BCA
c. Untuk dapat Mengetahui Ancaman Dan Risiko Yang akan Ditimbulkan Dari Keamanan Informasi Data Bank BCA
d. Untuk dapat Mengetahui Asesmen yang ada Terhadap Ancaman serta Risiko Informasi Data Bank BCA
e. Untuk dapat Mengetahui Risk Asesmen yang ada Terhadap Ancaman serta Risiko Informasi Data Bank BCA

KAJIAN TEORI

1. Definisi Keamanan Informasi

Keamanan Informasi adalah upaya untuk melindungi data perusahaan dan mencegah akses yang salah, perubahan program seperti pencurian dan kerusakan fisik pada sistem informasi, fungsi, prosedur dan tindakan teknis. Signifikansi nilai informasi hanya dapat diakses oleh orang-orang tertentu. Informasi yang diungkapkan kepada pihak lain dapat mengakibatkan kerugian bagi pemilik informasi.

Ada banyak perusahaan yang hanya diketahui oleh orang-orang tertentu saja, seperti informasi tentang produk yang sedang dikembangkan, algoritma dan teknik yang diperlukan untuk mendapatkan produk tersebut. Dalam keadaan ini, keamanan sistem informasi yang dilindungi dalam batas yang wajar diperlukan.

2. Tujuan Keamanan Informasi

Mengenai tujuan keamanan informasi diantaranya ialah sebagai berikut:

a. Confidentiality, merupakan bagian yang menjaga kerahasiaan informasi atau data dan memastikan bahwa hanya pihak-pihak terkait yang memiliki akses terhadap informasi tersebut.
b. Integrity, adalah bagian yang melindungi informasi agar infromasi tidak dapat diubah tanpa persetujuan data, menjamin keutuhan data dan mencakup kerusakan dan ancaman dari pihak lain yang dapat menyebabkan perubahan atau kegagalan data asli atau informasi
c. Availability, adalah bagian ketersediaan yang memastikan bahwa informasi siap saat dibutuhkan dan melindungi pengguna dari akses gratis ke data.

3. Manajemen keamanan informasi

Manajemen diharapkan tidak hanya memastikan keamanan aset informasi, tetapi juga memungkinkan perusahaan untuk melanjutkan perannya setelah terjadi bencana atau pelanggaran sistem keamanan. Kegiatan yang ditujukan untuk melindungi perusahaan dan aset informasi dikenal sebagai manajemen keamanan informasi.

Pada bentuknya yang paling dasar, manajemen keamanan informasi terdiri atas empat tahap, yaitu sebagai berikut:

a. Mengenali ancaman yang bisa menyerang sumber daya informasi perusahaan
b. Mengenali risiko yang bisa disebabkan oleh ancaman tersebut
c. Menetapkan kebijakan keamanan informasi
d. Menerapkan Asesmen agar dapat mengatasi risiko tersebut
e. Menerapkan Risk Asesmen agar dapat mengatasi risiko tersebut

4. Resiko Keamanan Informasi

Aktivitas tidak legal yang mengakibatkan risiko bisa diategorikan kedalam 4 jenis, diantaranya sebagai berikut:

a. Penggelapan serta penyingkapan data yang tidak legal
b. pengaplikasian sistem yang tidak legal ataupun orang yang tidak berhak mendapat akses informasi tersebut
c. Sabotase serta penyangkalan layanan yang tidak legal
d. Modifikasi data yang tidak legal

5. Keamanan Informasi pada PT Bank Central Asia

BCA secara historis mengamati evolusi teknologi cloud, yaitu penggunaan teknologi informasi melalui Internet, misalnya dalam penyimpanan informasi dan penggunaan aplikasi. BCA melihat peluang untuk memanfaatkan teknologi cloud dan memperluas beberapa rencana percontohan TI baru yang berpotensi mendukung bisnis bank. BCA juga mengumpulkan big data yang dapat mendukung analisis berbagai data untuk mengembangkan produk dan layanan sesuai permintaan nasabah. Big data merupakan salah satu teknologi terapan yang dibutuhkan untuk menganalisis data dalam jumlah besar. Saat ini BCA sedang mendesain ulang konsep big data, teknologi infrastruktur big data, dan software manajemen data, yang memungkinkan BCA mentransformasikan data dari sistem data warehouse tradisional menjadi sistem big data dan menambahkan data pendukung lainnya.

Demi menjaga kepercayaan nasabah dalam menggunakan layanan perbankan BCA, keamanan bertransaksi menjadi salah satu prioritas utama BCA. Oleh karena itu, dengan berkembangnya teknologi dan internet, ancaman kejahatan dunia maya dan kemungkinan penipuan semakin meningkat. Oleh karena itu BCA selalu menggunakan sistem keamanan IT yang handal dan berkelas internasional untuk mencegah ancaman cybercrime dan mendeteksi kejadian yang mencurigakan.

BCA akan terus menyediakan sistem keamanan bertransaksi di semua jaringan, termasuk jaringan perbankan online. Titik terlemah dalam pemasaran media online adalah Komputer/perangkat digital yang digunakan pelanggan mudah terinfeksi malware. Oleh karena itu, untuk mendeteksi risiko pencurian dan penyalahgunaan informasi, BCA memiliki sistem yang dapat mendeteksi malware pada komputer nasabah saat terhubung dengan jaringan perbankan online BCA. Pada tahun 2017, Bank BCA membentuk unit khusus (Tim Pusat Pemantauan Keamanan) yang bertugas memeriksa laporan sistem deteksi serangan dan malware serta memantau tindakannya yang diperlukan untuk melindungi keamanan sistem dan jaringan BCA. Manfaat Peningkatan Kesadaran Keamanan Informasi Bank BCA proaktif mengedukasi nasabahnya akan pentingnya menjaga kewaspadaan dalam bertransaksi.

Selain itu, karyawan internal disosialisasikan untuk memastikan keamanan kerja, termasuk menjaga kerahasiaan informasi. Penyempurnaan sistem manajemen nama pengguna dan hak akses, serta pembaruan rutin aplikasi keamanan seperti antivirus dan sistem pencegahan intrusi (IPS) untuk selalu memastikan keamanan jaringan.

METODE PENELITIAN

Metode penelitian artikel ilmiah ini menggunakan metode kualitatif seperti halnya penelitian literatur atau penelitian kepustakaan. Meliputi literatur, khususnya di bidang keamanan PT Bank BCA, menurut teori yang dikritik. Bank BCA. Selain itu juga dianalisis artikel ilmiah bereputasi dan artikel ilmiah dari jurnal belum bereputasi. Semua artikel ilmiah yang dikutip berasal dari Mendeley dan juga dari Google Scholars.

Dalam penelitian kualitatif ini, tinjauan literatur harus digunakan secara konsisten dengan adanya asumsi metodologis. Artinya harus digunakan secara induktif agar tidak mengarah pada pertanyaan yang diajukan peneliti. Alasan utama dilakukannya penelitian kualitatif adalah penelitian ini bersifat eksploratif (Ali & Limakrisna, 2013).

Kemudian dibahas secara rinci pada bagian “Literature Related” atau “Literature Review” sebagai dasar untuk merumuskan hipotesis dan juga sebagai dasar untuk penelitian selanjutnya melakukan perbandingan dengan hasil dan temuan penelitian (Ali & Limakrisna, 2013).

HASIL DAN PEMBAHASAN

1. Histori sekuriti

Dengan pesatnya teknologi informasi saat ini, interaksi nasabah secara digital dengan Bank BCA juga meningkat secara signifikan. Hal ini mengakibatkan risiko kejahatan teknologi, sehingga Bank BCA harus terus meningkatkan sistem keamanan TI-nya.

Tujuan pengembangan sistem keamanan Teknologi Informasi BCA adalah untuk memastikan keamanan informasi dan memastikan sistem teknologi informasi selalu siap menghadapi kejadian nasabah, termasuk pencegahan dan antisipasi kejahatan dunia maya dan kemungkinan penipuan.

Data Loss Prevention (DLP) merupakan strategi pengamanan informasi yang terus dilakukan Bank BCA untuk meningkatkan keamanan data elektronik penting terhadap pencurian data atau akses tanpa izin. Untuk memastikan keamanan penggunaan aplikasi internal Bank BCA yang terkoneksi dengan internet, Bank BCA dapat menggunakan pengamanan tambahan berupa two-factor authentication untuk memastikan bahwa aplikasi tersebut dapat diakses oleh orang yang tepat.

BCA mengimplementasikan solusi klasifikasi data untuk memastikan semua data perusahaan terklasifikasi sesuai dengan tingkat sensitivitas data. Bank BCA menggunakan solusi Database Monitoring untuk memastikan bahwa orang dan aplikasi yang tepat sedang mengakses database. Solusi ini dilengkapi dengan pembelajaran mesin dan kecerdasan buatan untuk memastikan tidak terjadi anomali. Untuk meningkatkan keamanan informasi rahasia terhadap database, Bank BCA menggunakan teknologi database masking yang mencegah pengungkapan informasi rahasia kepada pihak yang tidak berhak.

Bank BCA menjadi bank swasta pertama yang mendapatkan sertifikasi prestisius, yaitu sertifikasi Payment Card Industry Data Security Standard (PCI DSS) untuk seluruh lokasi yang mengelola transaksi dan data pemegang kartu, termasuk pusat data. Selain itu, Bank BCA juga mendapatkan sertifikat ISO 20000-1:2018 untuk meningkatkan service management system dan service management system (SMS). Untuk memastikan Bank BCA

memberikan layanan kepada setiap nasabah, Direktur TI juga memantau laporan berkala Strategic IT Group.

Selama tahun 2020, BCA memberikan pelatihan kesadaran rekayasa sosial melalui e-learning kepada seluruh karyawan BCA. Selain itu, tidak ada insiden signifikan terkait pelanggaran atau penyalahgunaan data dan privasi nasabah di BCA. Pada tahun 2020, tidak ada data pelanggan yang hilang. Dengan demikian, tidak ada sanksi/denda yang dikenakan kepada BCA atau karyawannya.

2. Protek sekuriti

BCA menggunakan teknologi enkripsi 2048-bit EV-SSL untuk melindungi data komunikasi antara komputer nasabah dengan server BCA pada saat nasabah menggunakan BCA KlikPay. Dapat memastikan perlindungan data komunikasi selama nasabah mengakses BCA KlikPay, nasabah juga bisa melakukan hal-hal sebagai berikut:

a. Periksa sertifikat SSL secara teratur untuk dapat memastikan bahwa nasabah menerima sertifikat SSL yang legal dan telah terdaftar untuk https://klikpay.klikbca.com.
b. Apabila nasabah menerima pesan yang menerangkan bahwa sertifikat tidak legal, maka nasabah dianjurkan untuk tidak melanjutkan akses terhadap situs BCA KlikPay.
c. Pastikan juga bahwa pada browser nasabah terdapat :
    - Gambar gembok/kunci yang sudah mengindikasikan bahwa halaman yang nasabah akses saat ini dienkripsi dengan menggunakan SSL. apabila nasabah tidak melihat gambar gembok/kunci, maka nasabah dianjurkan agar tidak melanjutkan akses terhadap situs BCA KlikPay serta pastikan juga alamat situs BCA KlikPay sudah benar.
    - Address bar berwarna hijau (selama Anda menggunakan versi terbaru browser yang kompatibel dengan EV SSL). Jika bilah alamat berwarna merah, klien tidak disarankan melanjutkan akses terhdap situs BCA KlikPay.
d. Pastikan juga bahwa nasabah sudah mengetik alamat yang benar yaitu https://klikpay.klikbca.com atau juga bisa melalui link BCA KlikPay pada www.klikbca.com ataupun melalui situs merchant yang sudah bekerja sama dengan BCA.
e. Pastikan juga bahwa nasabah sudah logout saat meninggalkan komputer nasabah walaupun hanya sesaat.

f. Sebaiknya nasabah tidak mengakses situs BCA KlikPay dari warnet ataupun jaringan yang tidak pasti keamanannya.

3. Antisipsi keamanan

BCA memiliki 3 (tiga) lapisan sistem pengamanan untuk dapat menjaga akses dan juga transaksi nasabah disitus BCA KlikPay yaitu :

a. Secure Socket Layer ("SSL")

   SSL adalah teknologi keamanan yang "mengenkripsi" jalur komunikasi antar komputer sehingga tidak dapat dibaca oleh pihak lain.

b. Password / kata sandi

c. Kode One Time Password (OTP) yang dihasilkan oleh sistem BCA

   Kode OTP adalah kata sandi yang dihasilkan oleh teknologi keamanan, yang selalu dapat menghasilkan kata sandi yang berbeda setiap kali Anda menggunakan perangkat keamanan.

Karena ada begitu banyak variasi browser Internet, cukup sulit untuk menawarkan layanan perbankan online yang menghargai keamanan masing-masing browser. Saat ini BCA hanya menawarkan layanan perbankan online yang lebih cocok untuk internet dengan Microsoft Internet Explorer versi 8 atau lebih tinggi.

Bank BCA menjaga kerahasiaan seluruh informasi dan data transaksi yang dimasukkan oleh nasabah di website BCA KlikPay sesuai dengan peraturan dan perundang-undangan yang berlaku di Indonesia dan kebijakan internal BCA. BCA juga memantau situs web komersial tempat koneksi pengguna berasal. kebutuhan penelitian. Website BCA KlikPay hanya dapat diakses dari website merchant yang telah bermitra dengan BCA atau dari website BCA sendiri. Selama pelanggan login ke website BCA KlikPay, BCA akan tetap menggunakan cookies yang akan kadaluarsa ketika pelanggan logout. Seluruh informasi transaksi website BCA KlikPay yang dilakukan oleh nasabah juga dicatat dan dijaga kerahasiaannya sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia dan kebijakan internal BCA.

4. Asesmen sekuriti

Berdasarkan penilaian keamanan teknologi dan informasi menggunakan sejumlah informasi yang diteliti antara lain:

a. Bahwasannya Bank BCA telah menggunakan sistem informasi dalam pemanfaatan teknologinnya.
b. Dilihat juga apakah telah mengacu pada tata kelola keamanan dalam penyelenggaraan layanan publik yang sudah dikeluarkan oleh kementriaan komunikasi serta informatika yang dilanjutkan oleh beberapa tahapan yang digunakan untuk rekomendasi yang sesuai dengan kondisi sistem informasi maupun teknologi informasi diinstusi.

5. Risk Asesmen Perusahaan

a. Identifikasi Resiko

Agar dapat melakukan identifikasi risiko, peneliti menggunakan metode document viewer.

Nama Risiko : Pembobolan ATM

Uraian Risiko

Paspor BCA nasabah digunakan oleh pihak yang tidak bertanggung jawab untuk bisa melakukan transaksi di ATM BCA.

Perkiraan Sumber Risiko

Penggunaan Skimer adalah alat untuk mengambil No Kartu Nasabah yang diletakakn di mulut mesin ATM serta menggunakan kamera pemantau agar mendapatkan PIN dari nasabah tersebut.

Uraian Dampak Risiko

Dampak yang ditimbulkan ialah pencurian dana nasabah oleh pihak yang tidak bertanggung jawab yang menimbulkan kerugian bagi para nasabah dan menurunya kepercayaan nasabah untuk melakukan transaksi di mesin ATM yang dapat menyebabkan kerugian yang tidak dapat diperbaiki di perbankan ritel.

Deskripsi potensi risiko

Risiko pembobolan ATM tinggi karena ATM tersebar di lokasi berbeda dan dijaga oleh satpam atau berada di area yang tidak dijaga oleh satpam.

kondisi berisiko

Risiko pembobolan ATM masih ada, bahkan bisa meningkat dengan moda transportasi lainnya..

b. Analisis Risiko

Analisis kemungkinan

Kriteria probabilitas:

Pembobolan ATM dengan skimmer sudah dilakukan sejak 2009, dan polisi menangkap satu komplotan. Namun, polisi dan bank setuju untuk merahasiakan penangkapan geng tersebut. Kejadian ini terjadi pada tahun 2010 dan telah merugikan 200 nasabah BCA. Dengan cara ini, kemungkinan risiko pembobolan ATM sesuai dengan level A, yang digambarkan hampir pasti.

Kriteria Dampak:

Selain berpotensi merugikan 200 nasabah BCA sebesar Rp5 miliar, pembobolan ATM juga dapat mengikis kepercayaan nasabah terhadap keamanan bertransaksi Menggunakan ATM bahkan bisa membuat nasabah menarik uang karena khawatir uangnya akan jatuh ke tangan penjahat. Dengan demikian, risiko pembobolan ATM juga dapat digolongkan high impact dengan nilai IV, karena tujuan penting tidak dapat dicapai.

Berdasarkan kriteria probabilitas level A dan klasifikasi kriteria dampak IV, dapat disimpulkan bahwa risiko pembobolan ATM memiliki klasifikasi risiko yang sangat tinggi.

Oleh karena itu, Risiko Pembobolan ATM membutuhkan penanganan yang cepat serta hati-hati, dan juga harus menyangkutpautkan dengan Manajemen Puncak.

PENUTUP

Kesimpulan

Kesimpulannya adalah bahwa keamanan informasi merupakan kebutuhan mutlak untuk semua bisnis, karena dengan keamanan informasi, bisnis dapat bekerja jauh lebih baik dan lebih efisien serta mengamankan informasi yang dimiliki bisnis. Digunakan oleh PT Bank Central Asia untuk menjaga kepercayaan nasabah terhadap perbankan BCA, BCA senantiasa mempergunakan sistem keamanan TI yang andal serta bertaraf internasional untuk mampu mencegah ancaman cybercrime dan mendeteksi aktivitas mencurigakan, serta BCA juga memiliki sistem yang dapat mendeteksi malware pada komputer nasabah saat terhubung melalui jaringan perbankan online BCA.

Di sisi lain, ancaman keamanan informasi dari sistem informasi adalah orang, organisasi, mekanisme atau kejadian yang dapat merusak sumber daya informasi perusahaan. Ancaman tersebut terdiri dari ancaman internal dan eksternal. Risiko keamanan informasi dapat didefinisikan sebagai pelanggaran keamanan informasi yang tidak diinginkan yang berpotensi disebabkan oleh ancaman keamanan informasi. Semua risiko adalah tindakan yang tidak sah.

DAFTAR PUSTAKA

Referensi dari Jurnal:

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

PT Bank Central Asia, 2017, Pemanfaatan teknologi informasi semakin berperan sebagai business enabler yang mendukung pertumbuhan bisnis yang berkelanjutan di BCA. Perkembangan teknologi informasi BCA diselaraskan dengan arah strategi serta kebijakan Bank

Putra, Y. M., (2019). Analysis of Factors Affecting the Interests of SMEs Using Accounting Applications. Journal of Economics and Business, 2(3). PUSTAKA

Anonim. 2017. Ancaman dan Keamanan Sistem Informasi Pada Bank BCA http://manajemen4b1.blogspot.com/2017/05/ancaman dan keamanan sistem informasi.html. Diakses pada 19 November 2019.