



Pengembangan Manajemen Sekuriti PT. Bank Central Asia (BCA)

Edy Soesanto¹, Chuck Noris Rupelu², Franco Nero Rupelu³, Alfian Saputra⁴

¹²³⁴Universitas Bhayangkara

Received: 20 Juni 2023
Revised: 28 Juni 2023
Accepted: 05 Juli 2023

Abstrak

Manajemen keamanan atau sikuriti menjadi penting dalam era digital saat ini. Dalam lingkungan bisnis yang kompleks dan terus berkembang, organisasi harus mengelola risiko keamanan informasi mereka dengan Cara yang sistematis dan efektif. Manajemen keamanan yang efektif memerlukan strategi, kebijakan, prosedur, dan kontrol yang tepat untuk melindungi aset informasi dari ancaman yang beragam, termasuk peretasan, virus, dan serangan siber lainnya. Manajemen keamanan atau sikuriti merupakan aspek penting dalam pengelolaan bisnis modern. Dalam era digital yang semakin kompleks, organisasi harus mempertimbangkan risiko keamanan yang beragam dan mengambil tindakan yang tepat untuk melindungi aset informasi mereka. Dengan menerapkan strategi yang tepat dan menggunakan kebijakan, prosedur, dan kontrol yang efektif, organisasi dapat meminimalkan risiko keamanan dan melindungi aset informasi mereka dengan cara yang efektif. Penelitian ini bertujuan untuk menganalisis dan meningkatkan manajemen sekuriti pada PT Bank Central Asia (BCA). Penelitian ini menggunakan pendekatan kualitatif dengan studi kasus pada PT BCA. Data dikumpulkan melalui pencarian informasi secara mendalam dari beberapa sumber berhubungan dengan manajemen keamanan serta analisis dokumen terkait manajemen sekuriti di perusahaan.

Keywords: Manajemen, Sekuriti, Manajemen sekuriti

(*) Corresponding Author: norisrupelu1234@gmail.com

How to Cite: Soesanto E., Rupelu C.N., Rupelu F.N., & Saputra A. (2023). Pengembangan Manajemen Sekuriti PT. Bank Central Asia (BCA). <https://doi.org/10.5281/zenodo.8149258>.

PENDAHULUAN

Manajemen sekuriti adalah suatu konsep atau praktik untuk memastikan keamanan dari sebuah sistem informasi dan data, serta melindungi informasi sensitif dari ancaman atau serangan yang mungkin terjadi. Tujuan utama manajemen sekuriti adalah untuk memastikan bahwa hanya orang yang berwenang yang memiliki akses ke informasi yang sensitif dan bahwa informasi tersebut tidak diubah atau diambil oleh orang yang tidak berwenang.

Manajemen sekuriti meliputi berbagai aspek, termasuk keamanan fisik, keamanan logis, manajemen risiko, dan pengendalian akses. Hal ini melibatkan implementasi kebijakan keamanan dan prosedur untuk melindungi aset organisasi, seperti informasi, perangkat keras, dan perangkat lunak, dari ancaman internal maupun eksternal.

Dalam praktiknya, manajemen sekuriti melibatkan penerapan teknologi keamanan informasi, seperti firewall, enkripsi, dan pengamanan jaringan. Namun, teknologi saja tidak cukup untuk memastikan keamanan yang optimal. Oleh karena itu, manajemen sekuriti juga melibatkan pendidikan dan pelatihan kepada karyawan mengenai kebijakan dan praktik keamanan informasi, serta audit dan pengawasan



terus menerus untuk memastikan bahwa kebijakan keamanan diikuti dan diperbarui sesuai dengan perkembangan teknologi dan ancaman keamanan yang baru.

Manajemen mengemukakan bahwa manajemen keamanan adalah suatu fungsi manajemen yang sangat penting dan harus dikelola secara efektif untuk melindungi organisasi dari risiko keamanan (Drucker, 2008).

Pembahasan tentang manajemen sekuriti fisik di dalam perusahaan yang diambil ialah di PT Bank Central Asia Tbk (disingkat BCA) (IDX: BBKA) 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.

BCA menawarkan berbagai produk dan layanan perbankan seperti tabungan, giro, deposito, pinjaman, kartu kredit, dan berbagai layanan perbankan digital seperti mobile banking, internet banking, dan ATM.

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.

Manajemen keamanan adalah suatu proses yang kompleks dan melibatkan banyak faktor, seperti teknologi, kebijakan, dan budaya organisasi (Schneier, 2008). Pada umumnya manusia sebagai individu pada dasarnya memiliki keinginan utama dalam hidup yaitu keinginan untuk mendapatkan makanan dan keinginan untuk mencukupi diri atau mempertahankan diri untuk bertahan hidup (Hadiman, 2008).

METODE

Manajemen adalah suatu proses yang melibatkan perencanaan, pengorganisasian, penggerakan, dan pengawasan untuk mencapai tujuan yang telah ditetapkan. Menurut para ahli, manajemen memiliki berbagai pengertian, seperti bekerja dengan orang-orang untuk menentukan, menginterpretasikan, dan mencapai tujuan (T. Hani Handoko), seni untuk menyelesaikan segala sesuatu (Peter F. Drucker), proses khas yang terdiri dari tindakan perencanaan, pengorganisasian, menggerakkan, dan pengawasan (Winardi), kemampuan mengarahkan dan mencapai hasil yang diinginkan dengan tujuan dari usaha-usaha manusia dan sumber daya lainnya (George R. Terry), dan lainnya. Karakteristik manajemen meliputi adanya tujuan, sumber daya, proses, pengambilan keputusan, dan pengaruh.

Keamanan informasi merupakan proses menghindari pengguna yang tidak berwenang mengakses, memakai, mengatakan, mengoperasikan, mengganti, ataupun menghancurkan data serta sistem data buat melindungi kerahasiaan, integritas, serta khasiat. 4 komponen membentuk keamanan data: organisasi, orang, proses, serta teknologi. Terdapat interaksi antara tiap- tiap budaya perbatasan, administrasi, arsitektur, penampilan, kebangkitan, serta sistem pendukung tidak hanya interaksi yang mengaitkan aspek manusia. Keamanan informasi merupakan aplikasi buat menghindari orang yang tidak berwenang menyalahgunakan pc, non-komputer, serta perlengkapan, informasi, serta data non- komputer. Penekanannya kerap kali pada fitur keras serta proteksi informasi sebab pemerintah serta bisnis mengakui perlunya melindungi peninggalan digital. Ungkapan "keamanan data"

begitu digunakan. Ruang lingkup yang terbatas ini setelah itu diperluas buat mencakup manusia dan fitur lunak, fitur keras, serta informasi (Agustina *et al.*, 2022).

Beberapa ahli seperti Michael E. Whitman dan Herbert J. Mattord memberikan pengertian tentang manajemen sekuriti. Manajemen keamanan meliputi kebijakan, prosedur, teknologi, dan orang-orang yang terlibat dalam melindungi informasi dan sumber daya penting.

Guna keamanan data melindungi informasi dari bermacam ancaman, menjamin kelangsungan bisnis, kurangi kerugian finansial untuk industri, serta memaksimalkan laba atas investasi serta prospek komersial. Sebab manajemen sistem data membolehkan informasi didistribusikan secara elektronik, dibutuhkan sistem buat menjamin kalau pengguna yang pas menerima serta mengirim informasi (Agustina *et al.*, 2022)

Kerahasiaan diperlukan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang (Whitman & Mattord, 2011).

Gagasan keamanan manusia menurut para ahli adalah bahwa keamanan tidak hanya terkait dengan keamanan nasional, tetapi juga melibatkan keamanan individu dan masyarakat. Keamanan manusia meliputi keamanan fisik, keamanan pangan, keamanan kesehatan, keamanan lingkungan, dan lain-lain. Para pendukung keamanan manusia menolak makna lama keamanan nasional dan berpendapat bahwa keamanan harus dilihat dari sudut pandang yang lebih luas, yaitu melindungi individu dan masyarakat dari berbagai ancaman yang dapat membahayakan keselamatan dan kesejahteraannya (Wikiwand, n.d.).

Penelitian ini menggunakan metodologi kualitatif, yang didefinisikan dengan pengumpulan data merata dari bermacam sumber yang dikira berarti di bidang keamanan. Pengumpulan informasi dicoba dengan tata cara observasi serta wawancara. Keputusan diambil sehabis informasi yang diperoleh sudah diproses serta dianalisis. buat mengumpulkan informasi yang dibutuhkan serta menggapai tujuannya, penulis menerapkan metode deskriptif pendekatan penelitian untuk menulis materi dalam penelitian ini untuk mengetahui masalah yang Akan terkait dengan pertanyaan yang diajukan dalam kaitannya dengan kebutuhan penulisan penulis.

Penelitian ini memiliki tujuan untuk mengetahui sistem manajemen sekuriti di PT. Bank Central Asia (BCA), untuk mengetahui kendala dalam penerapan sekuriti di PT. BCA dan untuk mengetahui pengembangan yang dilakukan dalam meningkatkan sekuriti di PT. BCA.

HASIL DAN PEMBAHASAN

BCA yang didirikan pada tahun 1957 dikala ini ialah bank swasta (non-publik) terbanyak di Indonesia dengan peninggalan senilai Rp1, 247 triliun serta modal bawah Rp122, 73 triliun per Desember 2022. Dengan modal ini 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

Sistem Pengamanan

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.

Proteksi Akses Situs BCA KlikPay

Untuk mengakses situs web BCA KlikPay, Anda harus memasukkan alamat email dan kata sandi Anda. Untuk memastikan perlindungan Anda saat mengunjungi website BCA KlikPay, mohon lakukan langkah-langkah berikut:

1. Jaga kerahasiaan kata sandi Anda. Jangan memberitahukan kata sandi Anda kepada orang lain atau memasukkan alamat email dan kata sandi Anda di halaman manapun kecuali website BCA KlikPay. Juga, jangan setuju untuk menggunakan alamat email dan kata sandi Anda di cache browser Anda selain situs web BCA KlikPay. Juga, jangan setuju untuk menggunakan alamat email dan kata sandi Anda di cache browser.

2. Jangan memberikan kata sandi Anda atau bagian dari kata sandi Anda kepada siapa pun, meskipun orang tersebut mengenali dirinya selaku pekerja BCA. BCA tidak sempat memohon kata sandi.
3. Administrasi Website BCA KlikPay – Ganti Kata sandi Anda secara berkala di menu ubah Kata sandi ataupun kalau Kamu mempunyai keraguan tentang keamanan kata sandi Kamu. Kata sandi yang tidak bermanfaat tercantum 111111, 222222, 123456, 654321, AAAAAA, BBBB, ulang tahun, no mobil, serta alamat. Jangan sempat menuliskan kata sandi Kamu di tempat yang bisa dilihat orang lain. Harap pakai kata sandi buat BCA- KlikPay yang berbeda dengan yang Kamu pakai buat masuk ke web website lain.

Harappakai kata sandi buat BCA- KlikPay yang berbeda dengan yang Kamu pakai buat masuk ke web website lain.

Proteksi Komunikasi BCA KlikPay

Dikala Kalian memakai BCA KlikPay, BCA melindungi koneksi antara pc Kamu serta server BCA memakai teknologi enkripsi 2048- bit EV SSL. Dikala memakai BCA KlikPay, Kamu bisa membenarkan proteksi komunikasi dengan melaksanakan perihal berikut::

1. Cek sertifikat SSL Kamu secara berkala buat membenarkan sertifikat tersebut aktif serta terdaftar di [https:// klikpay. klikbca. com](https://klikpay.klikbca.com).
2. Tidak dianjurkan buat memakai kembali web BCA KlikPay bila menerima notifikasi yang melaporkan sertifikat tidak berlaku.
2. Tidak dianjurkan buat senantiasa memakai web BCA KlikPay bila memandang pemberitahuan yang melaporkan sertifikat tidak benar.
3. Pastikan browser Anda memiliki
 - Bila Kamu memandang kunci gembok ataupun kunci, itu berarti enkripsi SSL lagi digunakan buat mengenkripsi Taman tempat Kamu terletak. Kamu dianjurkan buat menyudahi mengakses web BCA KlikPay serta cek kembali alamat web BCA KlikPay bila Kamu tidak bisa memandang key ataupun key image.
 - Bila Kamu memakai browser baru yang menunjang EV SSL, bilah alamat bercorak hijau. BCA tidak menganjurkan buat terus memakai web KlikPay bila URL bar bercorak merah.
4. Yakinkan alamat yang Kamu bagikan akurat. Itu wajib Lewat link BCA KlikPay di [www. clickbca. com](http://www.clickbca.com) ataupun di [https:// clickpay. clickbca. com](https://clickpay.clickbca.com) ataupun web website industri mitra
5. Matikan komputer tiap kali Kamu meninggalkannya, apalagi buat waktu yang pendek.
6. Jauhi mengakses web BCA KlikPay dari wifi publik ataupun jaringan dengan keamanan data yang diragukan.

Kode OTP (One Time Password)

BCA mensyaratkan penggunaan kode keamanan transaksi yang disebut kode OTP, yang dikirim oleh sistem BCA ke ponsel Anda sebagai layanan pesan teks. Kode OTP ini digunakan untuk mengotentikasi setiap pembelian online atau transaksi lainnya, yang menunjukkan bahwa Anda menyetujui transaksi tersebut.

Dikala melaksanakan transaksi pembayaran pembelian online ataupun transaksi yang lain, semacam: memandang profil BCA KlikPay aku(ubah

password, tambah/ hapus tata cara pembayaran, riwayat transaksi), kode OTP yang dihasilkan oleh sistem BCA wajib disertakan.

Menu Administrasi serta Dorongan sediakan transaksi yang bisa dituntaskan tanpa kode OTP.

Situs BCA KlikPay

Pada BCA bisa memposting tautan URL ke web website lain yang tidak terletak di dasar kendalinya di web website BCA KlikPay. Keamanan serta konten web website eksternal ini tidak terletak di dasar kendali BCA. Harap tinjau kebijakan pribadi serta keamanan web saat sebelum memakainya. Yakinkan URL yang Kamu pakai buat mengakses web BCA KlikPay Link BCA KlikPay dari [www. clickbca. com](http://www.clickbca.com) ada di [https:// clickpay. clickbca.com](https://clickpay.clickbca.com) pas bila Kamu mengaksesnya dengan meng- klik link dari web merchant yang bekerja sama dengan BCA. BCA berhak buat mengganti kebijakan pribadi serta keamanannya tiap dikala sehubungan dengan kondisi serta teknologi yang ada. Kamu senantiasa bisa memandang tipe terkini data serta kebijakan pribadi BCA di [www. klikbca. com/ klikpay](http://www.klikbca.com/klikpay) ataupun memohon salinannya lewat email halobca@bca.co.id.

Alamat Email dan Proteksi Informasi Transaksi

BCA butuh mengenali alamat email Kamu. Dikala awal kali bergabung, Kamu bisa menaikkan ataupun menghapus tata cara pembayaran, serta BCA memakai alamat email Kamu buat mengirimkan data tentang transaksi online yang dituntaskan memakai BCA KlikPay. Tidak hanya itu, Kamu menyetujui BCA memakai alamat email Kamu buat memberitahukan data, mengundang Kamu ke pertemuan, serta buat tujuan promosi yang lain. Buat menjamin keamanan informasi yang dikirimkan ke alamat email Kamu, jalani langkah- langkah berikut:

1. Masukkan alamat email pribadi Anda yang benar di BCA. Jangan gunakan alamat email yang salah.
2. Jika Anda mengubah alamat email, tutup BCA KlikPay.
3. Saat menghubungi BCA melalui email, jangan kirimkan informasi PIN, OTP, ataupun data berarti ataupun individu yang lain.

B. Risk Assasement Manajemen Sekuriti

Phishing

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:

- Membuat web website palsu yang mempunyai URL serta desain yang mirip dengan web website merchant BCA KlikPay ataupun BCA KlikPay yang legal.
 - Mengirimkan tautan URL ke web formal BCA KlikPay ataupun ke web website yang nampak mirip dengan web website BCA KlikPay, cuma buat mengenali kalau itu palsu
 - 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.
 - Berpura- pura jadi karyawan BCA serta memohon data dari Kamu.
- Ajuran pengamanan:

- Yakinkan Kamu mengakses www.klikbca.com/klikpay, web formal BCA KlikPay, dikala memakai BCA KlikPay. Simpan web di menu Kesukaan ataupun Bookmark supaya Kamu bisa dengan kilat memilihnya dari menu Kesukaan ataupun Bookmark pada kunjungan Kamu selanjutnya ke BCA KlikPay. Ini hendak menolong Kamu menghindari kesalahan pengetikan dikala memasukkan URL web BCA KlikPay. Beli secara eksklusif dari penjual BCA KlikPay. Pada menu/ web merchant BCA KlikPay, Kamu bisa menciptakan nama serta alamat web merchant BCA KlikPay
- Cek buat membenarkan kalau alamat web ataupun alamat yang diketik di bilah alamat browser Kamu merupakan yang ditampilkan di catatan orang dagang.
- Jika anda Yakinkan [https:// klikpay. klikbca. com](https://klikpay.klikbca.com) telah masuk di address bar browser bila Kamu mau memakai BCA KlikPay selaku opsi pembayaran buat transaksi online yang dicoba lewat web merchant BCA KlikPay.
- Yakinkan kode OTP SMS berasal dari pengirim 69888.
- Yakinkan nama transaksi, no transaksi, serta nama merchant pada SMS cocok dengan transaksi yang Kamu selesaikan.
- Yakinkan buat keluar dari komputer dikala Kamu meninggalkannya.
- Dianjurkan buat tidak memakai BCA KlikPay dari warnet ataupun jaringan yang tidak menjamin keamanan.
- Tidak diperkenankan memakai email, SMS, ataupun link terkirim yang lain buat mengakses web merchant BCA KlikPay ataupun web BCA KlikPay. Butuh dikenal kalau BCA tidak hendak mengirimkan email tersebut.
- Dilarang mengirimkan kode OTP kepada siapa juga, tercantum staf BCA. Was- was permintaan palsu buat data individu Kamu, semacam kata sandi BCA KlikPay ataupun kode OTP, yang terbuat oleh orang yang menyamar selaku pekerja BCA lewat telepon, faks, email, SMS, ataupun saluran yang lain.
- Jika Kirim email ke [halobca@bca. co. id](mailto: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.

Virus / Worm

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. Informasi hard disk hendak dihapus.
4. Tidak dapat memakai program aplikasi.

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.

Ajuran Keamanan:

- Gunakan antivirus terbaru di komputer Anda dan pastikan komputer Anda dipindai secara real time.
- Banyak virus dikirim melalui email, jadi berhati-hatilah saat menggunakan email. Hapus email mencurigakan atau email dari pengirim yang tidak dikenal dan pindai lampiran email sebelum membukanya.
- Gunakan firewall untuk sistem operasi komputer Anda atau instal firewall pribadi dan pastikan pengaturan firewall yang diinstal dapat melindungi komputer pribadi (PC) Anda.
- Kami menganjurkan agar Anda tidak mengakses atau mengunduh file atau program di Internet dari situs web yang tidak dikenal atau tidak tepercaya.
- Pindai file dari floppy disk, CD, atau drive USB yang masuk.
- Pastikan sistem pengoperasian dan aplikasi komputer Anda dilindungi oleh sistem keamanan terbaru.

Malware / Spyware

Suatu program komputer jahat, kerap diketahui selaku spyware, dirancang untuk " mencuri" informasi individu yang sensitif dari pc yang terinfeksi serta mengirimkannya ke tempat tertentu di Internet di mana pembuatnya nanti bisa mengambilnya kembali. No kartu kredit, ID pengguna serta PIN/ kata sandi, no rekening bank, serta alamat email merupakan sebagian contoh data sasaran yang sangat berarti.

Lewat lampiran email, program dari sumber tidak diketahui, ataupun web website" jahat", malware/ spyware bisa disebarkan.

Malware/ spyware bisa terbuat dari disebarkan oleh virus. Spyware bekerja di latar belakang serta tidak dikenal, tidak semacam virus, yang sifatnya lebih mengganggu, membuatnya lebih gampang untuk pembentuk/ distributor malware/ spyware untuk mengumpulkan informasi yang mereka butuhkan.

Ajuran Keamanan:

Proteksi terhadap virus serta worm identik dengan proteksi dari malware serta spyware.

Bot (roBot)

Bot adalah Robot, ataupun bot Bot yang diinstal merupakan tipe program komputer tertentu yang membolehkan pengguna lain untuk memanipulasi komputer Kamu dari jarak jauh lewat jaringan. Di Komputer Kamu, distributor serta produsen bot tidak dibatasi.

Umumnya, komputer yang dikendalikan, pula diketahui selaku botnet, digunakan untuk melanda pc lain yang tersambung ke jaringan ataupun mengirimkan spam, malware, serta worm.

Ajuran Keamanan:

Keamanan bot sama dengan pertahanan virus/ worm.

KESIMPULAN

Pengembangan sekuriti tidak hanya melibatkan teknologi, tetapi juga faktor manusia. Oleh karena itu, BCA juga melakukan pelatihan dan sosialisasi kepada

karyawan untuk meningkatkan kesadaran Akan pentingnya keamanan dan sekuriti dalam bisnis perbankan.

Pengembangan sekuriti PT Bank Central Asia menjadi sangat penting dalam menjaga kepercayaan nasabah dan mencegah terjadinya kebocoran data atau pencurian identitas. BCA telah melakukan berbagai upaya untuk meningkatkan keamanan sistem dan meningkatkan kesadaran karyawan. Namun, BCA harus terus melakukan inovasi dan pengembangan sistem keamanan dan sekuriti agar selalu dapat mengikuti perkembangan teknologi dan mengatasi ancaman keamanan yang terus berkembang.

DAFTAR PUSTAKA

- Agustina, D., Pramadista, F. N., & Regyna, T. F. (2022). *SISTEM MANAJEMEN KEAMANAN INFORMASI*.
- Drucker, P. (2008). *Pengertian Manajemen Menurut Para Ahli*.
<https://seputarilmu.com/2020/06/pengertian-manajemen-menurut-para-ahli.html>.
- Hadiman. (2008). *Manajemen Sekuritas*.
<https://id.scribd.com/document/346177549/Manajemen-Sekuriti>.
- Schneier, B. (2008). *Schenier on Security*.
- Whitman, M. E., & Mattord, H. J. (2011). *Keamanan Informasi*.
<https://mmsi.binus.ac.id/2017/11/17/Keamanan-Informasi/>.
- Wikiwand. (n.d.). *Keamanan Manusia*.
https://www.wikiwand.com/id/Keamanan_manusia.