**Makalah Keamanan Sistem Informasi**

**Model Arus Jaringan**

****

**Disusun oleh :**

Jervin descrates kontessa 51018013

**STMIK KHARISMA MAKASSAR**

**2020**

**Kata pengantar**

Puji syukur penulis panjatkan kehadirat Tuhan karena dengan rahmat, karunia, sehingga penulis dapat menyelesaikan makalah tentang “Keamanan Sistem Informasi”. Penulis berterima kasih Kepada dosen mata kuliah KSI(Keamanan Sistem Informasi) yang memberikan tugas ini.

Penulis sangat berharap makalah ini dapat berguna dalam menambah wawasan serta pengetahuan kita tentang Keamanan Sistem Informasi . Penulis juga menyadari bahwa di dalam makalah ini terdapat kekurangan dan jauh dari kata sempurna. Oleh sebab itu , penulis berharap adanya kritik, saran dan usulan demi perbaikan makalah yang telah penulis buat dimasa yang akan datang, mengingat tidak ada sesuatu yang sempurna tanpa saran yang membangun.

Semoga makalah yang sederhana ini dapat dipahami bagi siapapun yang membacanya. Sekiranya makalah yang telah disusun ini dapat berguna bagi penulis sendiri maupun orang yang membacanya. Sebelumnya penulis mohon maaf apabila terdapat kesalahan kata-kata yang kurang berkenan, dan memohon kritik dan saran yang membangun.

**DAFTAR ISI**

KATA PENGANTAR i

DAFTAR ISI ii

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Maksud dan tujuan 1

BAB II PEMBAHASAN

2.1 pengertian Jaringan 2

2.2permasalahan-permasalahan Model arus Jaringan dan contoh solusinya 2

BAB III PENUTUP

3.1 Kesimpulan 14

3.2 Kritik dan saran 14

Daftar pustaka 15

**BAB 1 PENDAHULUAN**

1.1 Latar Belakang

Di Era sekarang dimana teknologi yang sangat pesat membuat manusia dapat dengan mudah untuk menemukan informasi apapun di internet yang telah menghubungkan seluruh informasi yang ada di negara-negara lain, benua lain. Namun seiring perkembangan teknologi kita selalu ada ancaman pada keamanan sistem informasi kita yang agak berbahaya jika informasi ini jatuh ke tangan orang yang salah, namun kebanyakan menggunakan teknologi masih awam dengan “keamanan Sistem Informasi” oleh karena itu dengan adanya makalah ini dapat membuat mereka lebih memahami keamanan sistem informasi.

* 1. Rumusan Masalah

1. Apa yang dimaksud dengan Keamanan Sistem Informasi ?
2. Apa itu Analisis fundamental terkait perkembangan isu-isu keamanan sistem inforamsi saat ini ?
3. Bagaimana Implementasi keamanan sistem inforamsi diberbagai bidang ?
4. Apa saja peluang dan tantangan implementasi keamanan sistem informasi diberbagai bidang?
   1. Tujuan
5. Mengetahui dan memahami Keamanan Sistem Informasi.
6. Mengetaui perkembangan isu-isu keamanan sistem informasi.
7. Mengetahu implementasi keamanan Sistem Informasi di bidang tertentu.
8. Mengetahui peluang dan tentangan implementasi keamanan sistem informasi di bidang-bidang tertentu.

**BAB II PEMBAHASAN**

**2.1 Pengertian Keamanan Sistem Informasi**

Keamanan informasi (information security) digunakan untuk mendeskripsikan perlindungan baik peralatan Komputer dan non komputer dan non kompter, fasilitas, data, dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang.

Saat pemerintah dan kalangan industri menyadari kebutuhan untuk mengamankan sumber daya informasi mereka, perhatian nyaris terfokus secara eksklusif pada perlindungan peranti keras dan data, maka istilah keamanan sistem (system security) pun digunakan. Fokus sempit ini kemudian diperluas sehingga mencakup bukan hanya peranti keras dan data, namun juga peranti lunak, fasilitas komputer, dan personel. Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis (Chaeikar, etc., 2012).

Menurut (Whitman & Mattord, 2011) informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan.

Keamanan secara umum dapat diartikan sebagai ‘quality or state of being secure-to be free from danger’. Contoh tinjauan keamanan informasi sebagai berikut:

• Physical Security, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran

• Personal Security, strategi yang lebih memfokuskan untuk melindungi orang- orang dalam organisasi

• Operation Security, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman.

• Communications Security, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi.

• Network Security, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

Keamanan informasi adalah menjaga informasi dari ancaman yang mungkin terjadi dalam upaya menjamin kelangsungan bisnis, mengurangi tingkat risiko dan mempercepat atau memaksimalkan pengambilan keputusan investasi serta peluang bisnis. Tingkat keamanan pada informasi juga bergantung pada tingkat sensitifitas informasi dalam database, informasi yang tidak terlalu sensitif sistem keamanannya tidak terlalu ketat sedangkan untuk informasi yang sangat sensitif perlu pengaturan tingkat keamanan yang ketat untuk akses ke informasi tersebut.

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (cheating) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (right information), informasi dipegang oleh orang yang berwenang (right people), dapat diakses dan digunakan sesuai dengan kebutuhan (right time), dan memberikan informasi pada format yang tepat (right form).

**2.2 Implementasi KSI Pada Bidang Perusahaan bisnis**

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur- prosedur, struktur-struktur organisasi dan piranti lunak.

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai “*quality or state of being secure-to be free from danger”* [1]. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi memiliki fokus dan dibangun pada masing-masing ke-khusus-annya. Manajemen keamanan informasi pada Perusahaan memiliki tanggung jawab untuk program khusus, maka ada karakteristik khusus yang harus dimilikinya, yang dalam manajemen keamanan informasi dikenal sebagai 6P yaitu:

* Planning

Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

1) strategic planning yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,

2) tactical planning memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,

3) operational planning memfokuskan diri pada kinerja harian organisasi. Sebagi tambahannya, planning dalam manajemen keamanan informasi adalah aktifitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi. Ada beberapa tipe planning dalam manajemen keamanan informasi, meliputi :

* Incident Response Planning (IRP)

IRP terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam confidentiality, integrity atau availbilitysumberdaya informasi. Insident Response Planning meliputi incident detection, incident response, dan incident recovery.

* Disaster Recovery Planning (DRP)

Disaster Recovery Planning merupakan persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana. Pada beberapa kasus, insiden yang dideteksi dalam IRP dapat dikategorikan sebagai bencana jika skalanya sangat besar dan IRP tidak dapat lagi menanganinya secara efektif dan efisien untuk melakukan pemulihan dari insiden itu. Insiden dapat kemudian dikategorikan sebagai bencana jika organisasi tidak mampu mengendalikan akibat dari insiden yang terjadi, dan tingkat kerusakan yang ditimbulkan sangat besar sehingga memerlukan waktu yang lama untuk melakukan pemulihan.

* Business Continuity Planning (BCP)

Business Continuity Planning menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Identifikasi fungsi kritis organisasi dan sumberdaya pendukungnya merupakan tugas utama business continuity planning. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

* Policy

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

1. Enterprise Information Security Policy (EISP) menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
2. Issue Spesific Security Policy (ISSP) adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.
3. System Spesific Policy (SSP) pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

* Programs

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

* Protection

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (risk assessment) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

* People

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

* 1. **Implementasi KSI di bidang E-Business**

1. **Pengendalian akses dan keamanan**, Situs e-commerce harus memberikan rasa percaya dan akses yang aman untuk berbagai pihak dalam transaksi e-commerce, misalkan dengan adanya kata kunci (password), kunci enskipsi, sertifikasi, atau tanda tangan digital. Kemudian ada otorisasi akses yang hanya ke bagian tertentu saja sehingga hanya para pelanggan yang terdaftar saja yang dapat mengakses informasi dan aplikasi yang ada. Pengendalian akses dan keamanan ini perlu dilakukan untuk melindungi sumber daya situs e-commerce dari berbagai ancaman seperti peretas (hacker), pencurian password atau nomor kartu kredit, atau menghindari kegagalan sistem.
2. **Membuat profil dan personalisasi**, Proses pembuatan profil dan personilasasi menggunakan alat pembuat profil seperti pendaftaran, file cookie, software penelusur perilaku dalam situs web dan respon pemakai. Profil ini digunakan untuk mengenali kita sebagai pemakai individual, memberikan tampilan personalisasi, saran atas produk dan iklan web. Tujuan proses pembuatan profile ini untuk tujuan manajemen rekening, pembayaran, mengumpulkan data mengenai manajemen hubungan pelanggan, perencanaan pemasaran, dan untuk manajemen situs web itu sendiri.
3. **Manajemen pencarian**, Software e-commerce harus meliputi komponen mesin pencari situs web untuk dapat membantu para pelanggannya dalam menemukan produk dan jasa tertentu yang mereka inginkan untuk dievaluasi atau dibeli.
4. **Manajemen isi dan katalog**, Isi e-commerce sebagian besar berbentuk katalog multimedia yang memuat informasi produk sehingga membuat dan mengelola catalog merupakan rangkaian utama dari manajemen isi.Software manajemen isi tersebut bekerja dengan alat pembuat profile yang sudah disebutkan sebelumnya. Software manajemen isi akan membantu perusahaan e- commerce untuk mengembangkan, menghasilkan, mengirimkan, memperbaharui, dan menyimpan data teks serta informasi multimedia di situs web e-commerce. Selanjutnya manajemen isi dan katalog dapat diperluas untuk memasukkan proses konfigurasi produk yang akan mendukung layanan mandiri berbasis web dan penyesuaian massal atas berbagai produk perusahaan.
5. **Manajemen arus kerja, Sistem arus kerja e-business** digunakan untuk membantu para karyawan secara elektronik bekerja sama untuk menyelesaikan tugas pekerjaan dengan menggunakan mesin software arus kerja (workflow software engine). Sistem ini memastikan bahwa transaksi, keputusan, dan aktivitas kerja yang tepat dilakukan, serta data dan dokumen yang benar telah dikirimkan ke para karyawan, pelanggan, pemasok, dan pihak stakeholder.
6. **Pemberitahuan kegiatan**, Proses pemberitahuan kegiatan (event notification) memainkan peranan penting dalam sistem e-commerce karena sistem ini digunakan untuk memonitor semua proses e-commerce dan mencatat semua kegiatan yang relevan, termasuk perubahan mendadak atau ketika dalam masalah. Sistem ini akan memberitahukan kepada para pelanggan, pemasok, dan pegawai serta stakeholder mengenai semua kegiatan transaksi yang berkaitan dengan status mereka dengan melalui pesan elektronik seperti e-mail, newsgroup, penyeranta (pager), atau fax.
7. **Kerjasama dan perdagangan**, Tujuan utama e-commerce adalah untuk mendukung kesepakatan kerjasama dan layanan perdagangan yang dibutuhkan oleh para pelanggan, pemasok, dan stakeholder lainnya. Seperti halnya dalam e-business, sistem e-commerce juga fokus menumbuhkan komunitas berkepentingan online untuk meningkatkan layanan pelanggan dan membangun loyalitasnya.
8. **Proses pembayaran elektronik**, Pembayaran sebagai proses nyata dan penting dalam transaksi e-commerce. Sekarang ini sebagian besar sistem e-commerce yang terlibat dalam web dan bisnis B2C menggunakan proses pembayarannya dengan kartu kredit. Faktor Keberhasilan E-commerce Dalam Dunia Bisnis Dalam menciptakan perusahaan e-commerce yang sukses dan berkelanjutan maka secara umum tentunya perusahaan harus mencari cara untuk dapat membangun kepuasan, loyalitas, dan hubungan baik dengan para pelanggan secara online agar mereka tetap kembali ke toko web perusahaan kita. Kunci keberhasilan perusahaan ritel elektronik adalah ketika perusahaan mampu mengoptimalkan beberapa faktor sukses e-commerce seperti berikut:

* Selection and Value, Faktor Pilihan dan nilai meliputi pilihan produk yang menarik, harga yang bersaing, jaminan kepuasan, dan dukungan pelanggan setelah penjualan.
* Performance and Service, Faktor Kinerja dan pelayanan meliputi navigasi, proses belanja, dan pembelian serta konfirmasi pengiriman yang cepat dan mudah.Look and Feel, Faktor Tampilan dan rasa yakni meliputi pajangan web, situs web, area belanja, produk multimedia, halaman katalog dan fitur belanja yang menarik.
* Advertising and incentives, Faktor Iklan dan insentif meliputi : web dan promosi e-mail bersasaran serta penawaran khusus, termasuk iklan di berbagai situs afiliasi.
* Personal attention, Faktor perhatian personal meliputi halaman web personal, saran produk yang dipersonalisasi, iklan web dan pemberitahuan e-mail, serta dukungan interaktif untuk semua pelanggan.
* Community relationship, Faktor hubungan dengan komunitas meliputi komunitas virtual para pelanggan, pemasok, perwakilan perusahaan, dan lain-lainnya melalui newsgroup, ruang bincang, serta berbagai hubungan ke situs-situs terkait.
* Security and Reliability, Faktor keamanan dan keandalan meliputi keamanan informasi pelanggan dan transaksi di situs web, informasi produk yang dapat dipercaya, serta pemenuhan pesanan yang dapat diandalkan.
  1. **Implementasi KSI di bidang keamanan Bank BCA**

**Sistem pengaman pada Bank BCA**

Hampir seluruh perbankan di Indonesia sekarang ini telah memberikan pelayanan secara real time on line dalam bertransaksi. Peran teknologi dalam dunia perbankan sangatlah mutlak, dimana kemajuan suatu sistem perbankan sudah barang tentu ditopang oleh peran teknologi informasi. Semakin berkembang dan kompleksnya fasilitas yang diterapkan perbankan untuk memudahkan pelayanan, itu berarti semakin beragam dan kompleks adopsi teknologi yang dimiliki oleh suatu bank. Tidak dapat dipungkiri, dalam setiap bidang termasuk perbankan penerapan teknologi bertujuan selain untuk memudahkan operasional intern perusahaan, juga bertujuan untuk semakin memudahkan pelayanan terhadap customers.

# Analisis Sistem Informasi Manajemen pada Bank BCA

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.

# E-Commerce pada Bank BCA

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.

# Sumber Daya Komputasi dan Komunikasi yang Dimiliki Bank BCA

Dengan klik BCA, menyediakan bagi individu maupun pemilik bisnis berbagai layanan perbankan yang sesuai dengan kebutuhan mereka masing-masing melalui Internet. Sementara itu, bagi mereka yang selalu bepergian, disediakan jasa mobile banking melalui saluran-saluran m-BCA, SMS Top Up BCA, BCA by Phone dan Halo BCA. BCA telah mengembangkan infrastruktur broadband nirkabel untuk menjamin komunikasi data berkecepatan tinggi di antara kantor pusat dan kantor-kantor cabang..

Di tanggal 31 Maret 2010, para nasabah BCA dapat menghubungi 889 kantor cabang di seluruh Indonesia di samping dua kantor perwakilan di Hong Kong dan Singapura. Jasa- jasa khusus bagi pelanggan premium BCA Prioritas BCA juga tersedia di 130 kantor cabang. Di tingkat international, kami bekerja sama dengan lebih dari 1.831 bank koresponden di 108 negara guna menyediakan jasa-jasa seperti Perintah Pembayaran (Payment Order).

# Intranet dan Ekstranet

Intranet adalah jaringan komputer-komputer yang saling tersambung digunakan suatu sistem organisasi. Atau bisa dikatakan Intranet adalah LAN yang menggunakan standar komunikasi dan segala fasilitas Internet, diibaratkan berinternet dalam lingkungan lokal. umumnya juga terkoneksi ke Internet sehingga memungkinkan pertukaran informasi dan data dengan jaringan Intranet lainnya (Internetworking) melalui backbone Internet.

Ekstranet merupakan Penerapan teknologi internet dalam ruang lingkup beberapa perusahaan yang merupakan mitra satu sama lain, dengan kata lain Menghubungkan ke perusahaan partner dan supplier membutuhkan biaya yang tinggi dan tingkat kesulitan yang tinggi pula. Selain itu, dibutuhkan sering terjadi masalah dengan kompatibilitas device yang digunakan tiap perusahaan.

Penggunakan sistem informasi manajemen dalam operasional Bank BCA ini menghasilkan sesuatu yang positif demi kelangsungan berjalannya sistem perbankan, dampak positif tersebut diantaranya: Sistem informasi meningkatkan efisiensi dan produktivitas cabang, Memudahkan komunikasi antar cabang dengan adanya fasilitas E- mail, Layanan E-Commerce BCA berdampak positif bagi kebutuhan para merchant dalam meningkatkan penjualan dan menggarap potensial market yang lebih luas

Dengan memanfaatkan teknologi dan sumber daya manusia yang sangat terlatih, BCA telah berhasil memperluas jaringannya baik jaringan konvensional maupun elektronis untuk memberikan pengalaman perbankan yang paling nyaman bagi para nasabah

Kemudahan Nasabah dalam Mengaksses informasi: Bank BCA telah memakai teknologi yang strategis, dan penggunaan teknologi yang canggih secara tepat telah menjadi unsur penting dalam kekuatan kompetitif Bank BCA. Dengan teknologi ini, Bank BCA mengupayakan kemudahan nasabah Bank BCA untuk mengakses informasi tentang apa saja mengenai Bank BCA, sehingga nasabah dengan mudahnya memperoleh informasi yang mereka ingnkan tersebut.

Dengan sistem intranet dan ekstranet yang diterapkan BCA. Sebagai contoh, melalui layanan I-Banking BCA atau melalui ATM BCA para nasabah dapat secara langsung membayar rekening listrik atau telepon tanpa harus mendatangi PLN atau pun Telkom.

Selain dampak positif, dampak negatif akan ditimbulkan oleh penggunaan SIM pada Bank BCA, ini biasanya terjadi diantaranya Bank BCA akan kehilangan kepercayaan dari para konsumen yang disebabkan karena berbagai macam, diantaranya penggunaan teknologi internet yang kerap dengan namanya pembobolan sistem oleh seorang hacker, pembobolan sistem informasi manajemen ini bisa berlangsung dan berdampak yang besar bagi perusahaan karena sumber-smber informasi penting telah dicuri,

Yang kedua, Bank BCA bisa kehilangan kepercayaan dari para pelangan karena kesalahan sistem pada website miliknya, biasanya karena website yang kurang diupdate atau karena gangguan sistem, sehingga konsumen akan kesulitan untuk mendapatkan informasi yang jelas serta up to date dari Bank BCA. Padahal informasi ini sangat penting untuk menarik para konsumen.

Yang terakhir dampak negatif dari penggunaan sistem informasi manajemen pada Bank BCA adalah kerugian yang tidak terduga, disebabkan oleh ganguan yang disebabkan secara sengaja, ketidakjujuran, praktek bisnis yang tidak benar, kesalahan faktor manusia atau kesalahan sistem elektronik. Ekstranet merupakan Penerapan teknologi internet dalam ruang lingkup beberapa perusahaan yang merupakan mitra satu sama lain, dengan kata lain Menghubungkan ke perusahaan partner dan supplier membutuhkan biaya yang tinggi dan tingkat kesulitan yang tinggi pula. Selain itu, dibutuhkan sering terjadi masalah dengan kompatibilitas device yang digunakan tiap perusahaan, ini merupakan dampak negative yang ditimbulkan pada penggunaan system informasi manajemen pada Bank BCA.

# Sistem Keamanan E-Banking pada Bank BCA

1. Confidentiality

Aspek confidentiality memberi jaminan bahwa data-data tidak dapat disadap oleh pihak-pihak yang tidak berwenang. Serangan terhadap aspek ini adalah penyadapan nama account dan PIN dari pengguna Internet Banking. Penyadapan dapat dilakukan pada sisi terminal (komputer) yang digunakan oleh nasabah atau pada Jaringan (network menghindari adanya fraud yang dilakukan dari dalam (internal).

1. Integrity

Aspek integrity menjamin integritas data, dimana data tidak boleh berubah atau diubah oleh pihak-pihak yang tidak berwenang. Salah satu cara untuk memproteksi hal ini adalah dengan menggunakan checksum, signature, atau certificate. Mekanisme signature akan dapat mendeteksi adanya perubahan terhadap data. Selain pendeteksian (dengan menggunakan checksum, misalnya) pengamanan lain yang dapat dilakukan adalah dengan menggunakan mekanisme logging (pencatatan) yang ekstensif sehingga jika terjadi masalah dapat dilakukan proses mundur (rollback).

1. Authentication

Authentication digunakan untuk meyakinkan orang yang mengakses servis dan juga server (web) yang memberikan servis. Mekanisme yang umum digunakan untuk melakukan authentication di sisi pengguna biasanya terkait dengan:MNJ

* Sesuatu yang dimiliki (misalnya kartu ATM, chipcard)
* Sesuatu yang diketahui (misalnya userid, password, PIN, TIN)
* Sesuatu yang menjadi bagian dari kita (misalnya sidik jari, iris mata)

Salah satu kesulitan melakukan authentication adalah biasanya kita hanya) yang mengantarkan data dari sisi nasabah ke penyedia jasa Internet Banking. Penyadapan di sisi komputer dapat dilakukan dengan memasang program keylogger yang dapat mencatat kunci yang diketikkan oleh pengguna. Penggunaan keylogger ini tidak terpengaruh oleh pengamanan di sisi jaringan karena apa yang diketikkan oleh nasabah (sebelum terenkripsi) tercatat dalam sebuah berkas. Penyadapan di sisi jaringan dapat dilakukan dengan memasang program sniffer yang dapat menyadap data-data yang dikirimkan melalui jaringan Internet. Pengamanan di sisi network dilakukan dengan menggunakan enkripsi. Teknologi yang umum digunakan adalah Secure Socket Layer (SSL) dengan panjang kunci 128 bit.

Pengamanan di sisi komputer yang digunakan nasabah sedikit lebih kompleks. Hal ini disebabkan banyaknya kombinasi dari lingkungan nasabah. Jika nasabah mengakses Internet Banking dari tempat yang dia tidak kenal atau yang meragukan integritasnya seperti misalnya warnet yang tidak jelas, maka kemungkinan penyadapan di sisi terminal dapat terjadi. Untuk itu perlu disosialisasikan untuk memperhatikan tempat dimana nasabah mengakses Internet Banking. Penggunaan key yang berubah-ubah pada setiap sesi transaksi (misalnya dengan menggunakan token generator) dapat menolong. Namun hal ini sering menimbulkan ketidaknyamanan.Sisi back-end dari bank sendiri harus diamankan dengan menggunakan Virtual Private Network (VPN) antara kantor pusat dan kantor cabang. Hal ini dilakukan untuk menggunakan userid/account number dan password/PIN. Keduanya hanya mencakup satu hal saja (yang diketahui) dan mudah disadap. Pembahasan cara pengamanan hal ini ada pada bagian lain. Sementara itu mekanisme untuk menunjukkan keaslian server (situs) adalah dengan digital certificate. Sering kali hal ini terlupakan dan sudah terjadi kasus di Indonesia dengan situs palsu “kilkbca.com”. Situs palsu akan memiliki sertifikat yang berbeda dengan situs Internet Banking yang asli.

1. Non-repudiation

Aspek nonrepudiation menjamin bahwa jika nasabah melakukan transaksi maka dia tidak dapat menolak telah melakukan transaksi. Hal ini dilakukan dengan menggunakan digital signature yang diberikan oleh kripto kunci publik (public key cryptosystem). Mekanisme konfirmasi (misal melalui telepon) juga merupakan salah satu cara untuk mengurangi kasus. Penggunaan logging yang ekstensif juga dapat mendeteksi adanya masalah. Seringkali logging tidak dilakukan secara ekstensif sehingga menyulitkan pelacakan jika terjadi masalah. (Akses dari nomor IP berapa? Terminal yang mana? Jam berapa? Apa saja yang dilakukan?)

1. Availability

Aspek availability difokuskan kepada ketersediaan layanan. Jika sebuah bank menggelar layanan Internet Banking dan kemudian tidak dapat menyediakan layanan tersebut ketika dibutuhkan oleh nasabah, maka nasabah akan mempertanyakan keandalannya dan meninggalkan layanan tersebut. Bahkan dapat dimungkinkan nasabah akan pindah ke bank yang dapat memberikan layanan lebih baik. Serangan terhadap availability dikenal dengan istilah Denial of Service (DoS) attack. Sayangnya serangan seperti ini mudah dilakukan di Internet dikarenakan teknologi yang ada saat ini masih menggunakan IP (Internet Protocol) versi 4. Mekanisme pengamanan untuk menjaga ketersediaan layanan antara lain menggunakan backup sites, DoS filter, Intrusion Detection System (IDS), network monitoring, DisasterRecovery Plan (DRP), Business Process Resumption. Istilah- istilah ini memang sering membingungkan (dan menakutkan). Mereka adalah teknik dan mekanisme untuk meningkatkan keandalan.

1. Metode Keamanan

Layanan ini menggunakan beberapa metode keamanan terkini seperti:

1. Penggunaan protokol Hyper Text Transfer Protokol Secure (HTTPS), yang membuat pengiriman data dari server ke ISP dan klien berupa data acak yang terenkripsi.
2. Penggunaan teknologi enkripsi Secure Socket Layer (SSL) 128 bit, dari Verisign. Dengan SSL inilah, transfer data yang terjadi harus melalui enkripsi SSL pada komunikasi tingkat socket.
3. Penggunaan user ID dan PIN untuk login ke layanan Internet Banking ini.
4. Penggunaan metode time out session, yang menyebabkan bila setelah 10 menit nasabah tidak melakukan aktivitas apapun, akses tidak berlaku lagi.
5. Penggunaan PIN untuk setiap aktivitas perbankan. PIN ini di-generate dari Token PIN.

**2.5 Peluang dan tantangan implementasi keamanan sistem informasi diberbagai bidang**

1. **Peluang dan Tantangan di bidang perusahaan bisnis**

Tnntangan Implementasi KSIi di perusahaan bisnis adalah adanya Ancaman

Ancaman keamanan sistem informasi adalah orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan.

1. Ancaman Internal

Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut.

2. Ancaman Eksternal

Misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan kita atau disebut juga pesaing usaha.

Peluang Implementasi KSI di perusahaan bisnis adalah dapat meningkatkan menjaga sumber daya informasi perusahaan dengan aman, namn jga diharapkan untuk menjaga persahaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan. Aktifitas untuk menjaga agar perusahaan dan sumber daya informasi tetap aman disebut Manajemen keamanan informasi.

1. **Peluang dan Tantangan di bidang E-Business**

Peluang dan Tantangan Penggunaan e-commerce Dalam Dunia Bisnis

Dalam banyak kasus, sebuah perusahaan e-commerce bisa bertahan tidak hanya mengandalkan kekuatan produk saja, tapi dengan adanya tim manajemen yang handal, pengiriman yang tepat waktu, pelayanan yang bagus, struktur organisasi bisnis yang baik, jaringan infrastruktur dan keamanan, desain situs web yang bagus, beberapa faktor yang termasuk:

* 1. Menyediakan harga kompetitif
  2. Menyediakan jasa pembelian yang tanggap, cepat, dan ramah.
  3. Menyediakan informasi barang dan jasa yang lengkap dan jelas.
  4. Menyediakan banyak bonus seperti kupon, penawaran istimewa, dan diskon.
  5. Memberikan perhatian khusus seperti usulan pembelian.
  6. Menyediakan rasa komunitas untuk berdiskusi, masukan dari pelanggan, dan lain-lain.
  7. Mempermudah kegiatan perdagangan.

E-commerce memberikan pilihan kepada produsen tentang jenis usaha dan skala usaha yang akan dikembangkan. Dengan mengimplementasikan teknologi informasi E- commerce, produsen dapat memilih untuk mengembangkan target pasar kepada pasar global atau hanya fokus terhadap segmen pasar tertentu. Bagi usaha kecil dan menengah, dengan menggunakan e-commerce dapat menawarkan sesuatu yang berkualitas dan terjangkau serta memiliki kepercayaan diri menghadapi pesaing yang menjadi tantangan dan juga tantangan lainnya yang sudah wajib dimiliki oleh semua pelaku e-commerce adalah Menjamin Keamanan Sistem Informasi agar tak bisa disalah gunakan oleh orang yang menyalah gunakan contohnya seperti kasus yang baru – baru ini terjadi Disalah satu perusahaan E-commerce yang data pengguna atau data pribadi user semua telah bocor atau terpublikasi hal ini yang merupakan tantangan yang wajib di atasi.

**Peluang dan Tantangan di bidang keamanan informasi bank BCA**

1. Interruption  -> informasi dan data yang ada dalam sistem komputer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.

2. Interception -> informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses ke komputer dimana informasi tersebut disimpan.

3. Modifikasi -> orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.

4. Fabrication -> orang yang tidak berhak berhasil meniru suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

1. **Mempercepat arus informasi**

Arus informasi saat ini menjadi sangat cepat, bahkan cenderung tidak terkontrol hingga saat ini. namun demikian, hal ini merupakan salah satu dampak positif, karena dapat memberikan informasi mengenai suatu kejadian secara cepat, meskipun terkadang tidak akurat dan tidak tepat.

Arus informasi dengan feedback yang merupakan [karakteristik sistem informasi](https://dosenit.com/kuliah-it/sistem-informasi/karakteristik-sistem-informasi)menjadi salah satu faktor perkembangan informasi dan komunikasi yang tampak. Sehingga memberikan manfaat tersendiri bagi setiap user. Terlebih terhadap internet, [perkembangan jaringan komputer](https://dosenit.com/jaringan-komputer/perkembangan-jaringan-komputer) menjadi semakin pesat seiring penggunaan internet yang kian meningkat.

1. **Mempermudah akses terhadap informasi terbaru**

Merupakan salah satu efek domino dari bertambah cepatnya arus informasi. Dengan adanya teknologi informasi dan komunikasi yang berkembang sangat pesat, maka siapapun akan bisa memperoleh informasi dengan mudah. Akses terhadap informasi ini bisa dilakukan kapanpun, dimanapun, dan dari siapapun itu. Hal ini akan membantu individu dalam meningkatkan informasi dan pengetahuan yang dimilikinya, meski terkadang realibilitas dan validitas dari informasi tersebut dipertanyakan.

**BAB III Penutup**

* 1. Kesimpulan

Dapat disimpulkan bahwa Keamanan informasi (informationsecurity) 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.

**Daftar Pustaka**

W.Taylor III, Bernard. 2004. Introduction to management science 8th edition. Pearson Education: Prentice Hall, Putra, Yananto Mihadi. (2018). Modul Kuliah Sistem Informasi Manajemen: Implementasi Sistem Informasi.  FEB - Universitas Mercu Buana: Jakarta.

<https://jigokushoujoblog.wordpress.com/2010/11/20/pentingnya-manajemen-kontrol-keamanan-pada-sistem/>

<https://blogs.itb.ac.id/23215139gilangramadhanel5216mrkisem1t15d16mr/2015/11/30/manajemen-risiko-dalam-perspektif-positif-dan-negatif/>

<https://dosenit.com/kuliah-it/teknologi-informasi/dampak-positif-dan-negatif-penggunaan-teknologi-informasi-dan-komunikasi>

<https://sis.binus.ac.id/2015/07/01/resiko-dalam-penerapan-sistem-informasi-di-perusahaan/>

Putra, Y. M. (2018). Penggunaan Teknologi Informasi Pada E-Business. *Modul Kuliah Sistem Informasi Manajemen.* FEB-Universitas Mercu Buana: Jakarta".

Rahmati. 2009. Pemanfaatan E-commerce Dalam Bisnis Di Indonesia [http://citozcome.blogspot.com/2009/05/pemanfaatan-e-commerce-dalam-bisnis-di.html.](http://citozcome.blogspot.com/2009/05/pemanfaatan-e-commerce-dalam-bisnis-di.html) Diakses tanggal 06 Agustus 2011.