“SISTEM MANAJEMEN KEAMANAN INFORMASI”

Dian Agustina, Firania Nazzilla Pramadista,

Tatya Fara Regyna

ABSTRAK

Informasi adalah salah satu aset terpenting yang sangat berharga bagi kelangsungan hidup organisasi / bisnis, pertahanan keamanan dan integritas nasional, kepercayaan publik atau konsumen, sehingga ketersediaan, akurasi, dan integritas informasi. Anda perlu menjaga jenis kelamin Anda. Informasi dapat ditampilkan dalam berbagai format, termasuk: Contoh: teks, gambar, audio, video. Manajemen informasi penting untuk kredibilitas dan kelangsungan hidup massa. Tujuan dari manajemen informasi adalah untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi tersebut. Keamanan informasi bertujuan untuk memastikan kerahasiaan, ketersediaan, dan integritas semua aset informasi perusahaan, bukan hanya perangkat keras dan data.

Kata Kunci: Informasi, Manajemen Informasi, Sistem Keamanan Informasi, Manajemen Keamanan

ABSTRACT

Information is one of the most important assets that is very valuable for the survival of the organization / business, defense of national security and integrity, public or consumer trust, so the availability, accuracy and integrity of information. You need to take care of your gender. Information can be displayed in a variety of formats, including: Example: text, images, audio, video. Information management is essential to the credibility and survival of the masses. The purpose of information management is to protect the confidentiality, integrity and availability of such information. Information security aims to ensure the confidentiality, availability and integrity of all company information assets, not just hardware and data.

Keywords: Information, Information Management, Information Security System, Security Management

PENDAHULUAN

Latar Belakang

Semua organisasi perlu menjaga aset informasi mereka tetap aman. Industri telah lama menyadari kebutuhan untuk melindungi penjahat komputer, dan sekarang pemerintah telah meningkatkan tingkat keamanan mereka untuk memerangi terorisme, mereka perlu mengatasi masalah utama keamanan dan ketersediaan, serta keamanan dan privasi.

Informasi dan data adalah aset perusahaan. Keamanan data secara tidak langsung dapat menjamin kelangsungan bisnis, memitigasi risiko, mengoptimalkan laba atas investasi, dan menjajaki peluang bisnis. Semakin banyak informasi perusahaan disimpan, dikelola, dan dibagikan, semakin besar risiko kerusakan data, kehilangan, atau paparan pihak luar yang tidak diinginkan.

Di sini, peran keamanan informasi sangat penting untuk menjaga dan semakin memperkuat kepercayaan konsumen. Hal ini karena ketika kepercayaan pelanggan tumbuh, begitu pula perusahaan yang menyediakan layanan pelanggan. Untuk memastikan keamanan informasi terhadap semua kemungkinan ancaman, perusahaan perlu menerapkan perlindungan keamanan informasi.

Keamanan informasi didefinisikan sebagai melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan. Keamanan informasi terdiri dari empat bidang: organisasi, orang, proses, dan teknologi. Setiap perbatasan berinteraksi tidak hanya dalam hal faktor manusia, tetapi juga dalam hal budaya, manajemen, arsitektur, penampilan, revitalisasi dan dukungan.

Tujuan Penelitian

Tujuan penelitian ini untuk mengetahui sistem keamanan dalam mencegah ancaman terhadap sistem suatu perusahaan, seperti pencurian data, penggunaan sistem secara ilegal serta memperbaiki dan mendeteksi kerusakan yang terdapat pada sistem.

LANDASAN TEORI

A. Pengertian Sistem Informasi Manajemen

Menurut Slamet Hariyanto dalam (Hariyanto, 2016). Manajemen itu sendiri meliputi perencanaan, pengorganisasian, pemantauan, pengarahan, dan proses lainnya dalam organisasi. Informasi dalam suatu organisasi, di sisi lain, adalah data yang diproses dengan cara yang berharga dan bermakna bagi organisasi.

Menurut Miyarso Dwi Ajie dalam (Ajie, 1375). Sistem informasi manajemen bukanlah hal baru. Ruang lingkup SIM sebenarnya terkandung dalam tiga kata yang membentuk SIM: "sistem", "informasi", dan "manajemen".

Sistem adalah kumpulan dari elemen-elemen yang saling berhubungan. Elemen-elemen sistem adalah departemen internal seperti gudang bahan baku, gudang produk jadi, produksi, promosi dan penjualan, dan pihak eksternal seperti pemasok dan konsumen yang saling terkait.

Informasi adalah hasil pengolahan data yang diperoleh dari setiap elemen sistem ke dalam format yang mudah dimengerti dan mewakili pengetahuan yang relevan yang dibutuhkan orang untuk meningkatkan pengetahuan mereka tentang fakta-fakta yang ada.

Manajemen terdiri dari proses kegiatan yang dilakukan oleh para pemimpin bisnis, seperti: perencanaan, pengorganisasian, koordinasi, dan pengendalian operasi untuk mencapai tujuan yang telah ditetapkan.

Dari ruang lingkup di atas, beberapa definisi sistem informasi manajemen menurut para ahli adalah sebagai berikut:

1. Menurut Jogiyanto Hartono (2000:700), istilah sistem informasi terkelola adalah kumpulan sistem informasi yang saling berinteraksi yang bertanggung jawab untuk pemrosesan dan pengumpulan data, menyediakan informasi yang berguna untuk mengelola semua tingkat kegiatan perencanaan dan pengendalian.
2. Menurut Joel D. Aron (buku E.S. Margianti), Pengertian Sistem Informasi Manajemen adalah sistem informasi yang menyediakan informasi yang dibutuhkan manajer untuk mengambil keputusan.
3. Menurut James. AF Stoner (buku Mu'alimah) menyediakan sistem informasi manajemen dengan informasi yang tepat waktu, andal, dan andal yang dapat mendukung proses pengambilan keputusan untuk perencanaan, pemantauan, dan pengoperasian fungsi organisasi yang lebih efektif. Didefinisikan sebagai cara formal untuk menyediakan manajemen.
4. Menurut Raymond Coleman (diterjemahkan oleh Moekijat 1991: 40), konsep sistem informasi manajemen yang efektif adalah asosiasi yang akurat dan tepat waktu untuk perencanaan, analisis, dan pengendalian manajemen sistem untuk mengoptimalkan pertumbuhan bisnis, jika Anda dapat memberikan data. Dalam *(14 Pengertian Sistem Informasi Manajemen Menurut Ahli - Materi Dosen, n.d.)*

B. Pengertian Keamanan Informasi

Menurut Sarno dan Iffano dalam (Puriwigati & Buana, 2020). Keamanan informasi merupakan upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan Anda mengoptimalkan laba atas investasi. Menurut ISO/IEC 17799:2005 dalam (Puriwigati & Buana, 2020) tentang Sistem Manajemen Keamanan Informasi, keamanan informasi berasal dari berbagai ancaman untuk menjamin kelangsungan bisnis, meminimalkan risiko bisnis, serta meningkatkan investasi dan peluang bisnis.

Informasi merupakan aset yang sangat berharga bagi suatu organisasi karena merupakan salah satu sumber daya strategis untuk meningkatkan nilai bisnis dan kepercayaan publik. Oleh karena itu, perlindungan informasi (keamanan informasi)

adalah masalah mutlak dan harus dipertimbangkan secara serius di semua tingkat kepemilikan, kontrol, dan karyawan organisasi yang terlibat. Keamanan informasi yang dimaksud meliputi kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman yang dapat merugikan kelangsungan hidup organisasi Anda.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi antara lain:

1. Physical security adalah keamanan informasi yang berfokus pada strategi untuk melindungi individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman seperti bahaya kebakaran, akses tidak sah, dan bencana alam.
2. Personal security adalah keamanan informasi yang berkaitan dengan perlindungan pribadi, biasanya mengacu pada tingkat keamanan fisik.
3. Operasional security adalah keamanan informasi. Ini menyangkut strategi organisasi untuk memastikan bahwa ia beroperasi tanpa gangguan.
4. Communication security adalah keamanan informasi yang ditujukan untuk melindungi media komunikasi, teknologi komunikasi, dan hal-hal internal lainnya. Kemampuan menggunakan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. Network security adalah keamanan informasi yang berfokus pada perangkat jaringan, data organisasi Anda, cara Anda melindungi jaringan dan kontennya, dan kemampuan untuk menggunakan jaringan Anda untuk menjalankan fungsi komunikasi data organisasi Anda. Dalam (Intika & Buana, 2020).

PEMBAHASAN

A. Keamanan Informasi

Keamanan informasi digunakan untuk mewakili perlindungan komputer dan perangkat, peralatan, data, dan informasi non-komputer dan non-komputer dari penyalahgunaan oleh orang yang tidak berwenang. Karena pemerintah dan industri menyadari perlunya melindungi aset informasi, fokusnya paling sering pada perangkat keras dan perlindungan data. Oleh karena itu, istilah keamanan informasi digunakan. Fokus sempit ini kemudian diperluas untuk mencakup tidak hanya perangkat keras dan data, tetapi juga perangkat lunak, peralatan komputer, dan personel.

B. Kegunaan Keamanan Informasi

Keamanan informasi melindungi informasi dari berbagai ancaman, memastikan kelangsungan bisnis, meminimalkan kerugian perusahaan, dan memaksimalkan laba atas investasi dan peluang bisnis. Manajemen sistem informasi memungkinkan pendistribusian data secara elektronik, sehingga diperlukan suatu sistem untuk memastikan bahwa data dikirim dan diterima oleh pengguna yang benar.

Keamanan informasi ditujukan untuk melindungi aspek-aspek berikut:

1. Kerahasiaan adalah aspek memastikan kerahasiaan data atau informasi, membuat informasi hanya dapat diakses oleh orang yang berwenang, dan memastikan kerahasiaan data yang dikirimkan, diterima, dan disimpan.
2. Integritas adalah aspek yang mencegah data dimodifikasi tanpa izin dari pihak yang berwenang, proses menjaga keakuratan dan integritas informasi dan memastikan aspek integritas ini Metode.
3. Availability adalah aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan). Dalam (Syafriзал, 2007).

Keamanan informasi dicapai melalui penerapan set kontrol yang tepat yang dapat berupa kebijakan, praktik, prosedur, struktur organisasi, dan perangkat lunak.

C. Manajemen Keamanan Informasi

Manajemen diharapkan tidak hanya untuk melindungi aset informasi, tetapi juga untuk menjaga fungsi bisnis mereka setelah bencana atau runtuhnya sistem keamanan. Aktivitas melindungi perusahaan dan aset informasinya disebut manajemen keamanan informasi.

CIO adalah orang yang tepat untuk bertanggung jawab atas keamanan informasi, tetapi sebagian besar organisasi memulai dengan menunjuk orang tertentu yang dapat mengabdikan diri untuk kegiatan ini. Direktur keamanan sistem informasi perusahaan ditunjuk untuk mewakili individu dalam organisasi, biasanya anggota departemen sistem informasi yang bertanggung jawab atas keamanan sistem informasi perusahaan. Namun, dengan penunjukan Corporate Information Assurance Department Manager (CIAO), perubahan telah dilakukan untuk mencapai tingkat informasi yang lebih tinggi di dalam perusahaan. CIAO harus memiliki sejumlah sertifikasi keamanan dan setidaknya 10 tahun pengalaman dalam mengelola fasilitas keamanan informasi.

Dalam bentuknya yang paling dasar, manajemen keamanan informasi terdiri dari empat fase, yaitu:

1. Identifikasi ancaman yang dapat menyerang aset informasi perusahaan Anda
2. Identifikasi risiko yang dapat ditimbulkan oleh ancaman ini
3. Menentukan kebijakan keamanan informasi
4. Menerapkan manajemen untuk mengatasi risiko tersebut.

D. Ancaman dan Jenis Ancaman

1. Ancaman

Ancaman keamanan sistem informasi adalah orang, organisasi, mekanisme, atau peristiwa yang dapat merusak aset informasi organisasi. Ancaman dibedakan menjadi 2, yaitu:

a) Ancaman Internal

Ancaman internal tidak hanya mencakup karyawan perusahaan, tetapi juga pekerja agen, konsultan, kontraktor, bahkan mitra bisnis perusahaan.

b) Ancaman Eksternal

Misalnya, perusahaan lain yang memiliki produk yang sama dengan kita, atau dikenal juga sebagai pesaing bisnis. Dalam (Intika & Buana, 2020).

2. Jenis-Jenis Ancaman

Jenis ancaman dibagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif:

a) Ancaman Aktif mencakup:

1) Pencurian data

Jika informasi anda didatabase dan dapat diakses oleh orang yang tidak berwenang, maka anda dapat kehilangan informasi atau bisa juga uang. Misalnya musuh perusahaan membayar seorang mata-mata dan dapat memperoleh informasi rahasia perusahaan anda, penjahat computer atau hacker mencuri data penting perusahaan anda dan meminta imbalan berupa uang yang nominalnya sangat besar.

2) Penggunaan sistem secara legal

Penjahat komputer jenis ini biasanya adalah seorang hacker. Yaitu, orang-orang yang senang mendapatkan data dan informasi penting yang mereka butuhkan, mengakses sistem telepon, dan membobol sistem keamanan untuk melakukan panggilan jarak jauh ilegal.

3) Penghancuran data secara legal

Seseorang yang dapat merusak atau menghancurkan data atau informasi dan mematikan sistem operasi komputer. Penjahat komputer ini tidak harus berada di tempat kejadian. Itu dapat menyerang perangkat Anda melalui jaringan komputer Anda, merusak semua sistem Anda dan kehilangan data

dan informasi penting. Penjahat komputer jenis ini biasa disebut dengan cracker. Dengan kata lain, ini adalah cracker sistem komputer yang tujuannya adalah untuk mencuri data atau merusak sistem Anda.

4) Modifikasi secara legal

Perubahan-perubahan dalam data atau keterangan & aplikasi secara nir disadari. Jenis modifikasi yg menciptakan pemilik sistem sebagai resah lantaran adanya perubahan dalam data & aplikasi ditimbulkan sang program pelaksanaan yg Mengganggu (malicious software). Program pelaksanaan yg bisa Mengganggu tadi terdiri berdasarkan acara lengkap atau segemen kode yg melaksanakan fungsi yg nir dikehendaki sang pemilik sistem. Fungsi ini bisa menghapus arsip atau mengakibatkan sistem terhenti. Jenis pelaksanaan yg bisa Mengganggu data atau aplikasi yg paling terkenal merupakan virus. Dalam (Paryati, 2008).

b) Ancaman Pasif mencakup:

1) Kegagalan sistem

Inkonsistensi data dapat terjadi karena kesalahan sistem atau kesalahan perangkat lunak dan perangkat keras. Transaksi tidak berjalan lancar dan dapat mengakibatkan data tidak lengkap atau rusak. Selain itu, tegangan yang tidak stabil dapat merusak atau membakar perangkat.

2) Kesalahan manusia

Kesalahan operasi sistem antropogenik dapat membahayakan integritas sistem dan data.

3) Bencana alam

Bencana alam seperti gempa bumi, banjir, kebakaran, dan badai merupakan faktor tak terduga yang dapat mengancam sistem informasi dan kekurangan sumber daya untuk mendukungnya. Dalam (Paryati, 2008).

E. Risiko Keamanan Informasi

Ini didefinisikan sebagai keluaran potensial yang tidak diinginkan dari pelanggaran keamanan informasi karena ancaman keamanan informasi. Semua risiko mewakili penipuan. Risiko ini dapat dibagi menjadi empat jenis:

1. Interruption: Ancaman terhadap ketersediaan. Artinya, data dan informasi dalam sistem komputer rusak dan hancur, sehingga tidak ada atau tidak dapat digunakan.
2. Interception: Ancaman terhadap rahasia. Artinya, seseorang yang tidak berwenang mengakses informasi dalam sistem komputer.
3. Modificcation: Ancaman terhadap integritas. Ini berarti bahwa tidak hanya orang yang tidak berwenang dapat memperoleh akses, tetapi mereka juga dapat membuat perubahan pada informasi.
4. Fabrication: Kehadiran orang yang tidak berwenang untuk meniru atau merusak objek dalam sistem. Dalam (Intika & Buana, 2020).

F. Macam-Macam Pengendalian

1) Pengendalian Teknis

Ini adalah kontrol yang dibangun ke dalam sistem dan dibuat oleh produsen sistem selama siklus pengembangan sistem. Dilakukan dalam tiga fase:

a. Idendtitas Pengguna

Ini memberikan informasi yang Anda ketahui, seperti kata sandi dan nomor telepon. nomor telepon.

b. Otentikasi Pengguna.

Pengguna memverifikasi akses dengan memberikan apa yang mereka miliki, seperti chip identifikasi dan token.

c. Hak Pengguna

Anda dapat memberikan hak kepada pengguna untuk memasuki tingkat penggunaan tertentu. Ketika pengguna mencapai tiga tingkat ini, mereka akan dapat menggunakan sumber informasi yang termasuk dalam pembatasan akses file. Dalam (Intika & Buana, 2020).

2) Pengendalian Kriptografis

Penggunaan kode yang menggunakan proses matematika. Meningkatkan keamanan data dengan mengaburkan data dalam format yang tidak dapat dibaca. Membantu melindungi data dan informasi yang disimpan dan dikirimkan dari pengungkapan yang tidak sah.

Enkripsi dapat dibagi sebagai berikut:

a) Enkripsi simetris

Untuk enkripsi ini, kunci enkripsinya sama dengan kunci dekripsi.

b) Enkripsi asimetris

Dengan enkripsi, kunci enkripsi tidak sama dengan kunci dekripsi. Dalam (Intika & Buana, 2020).

3) Pengendalian Fisik

Peringatan pertama dari penyusupan adalah mengunci pintu ruang komputer. Perkembangan lebih lanjut telah menghasilkan kunci yang lebih canggih yang dapat dibuka dengan tagihan, cetakan suara, kamera pengintai, dan perangkat keamanan.

4) Pengendalian Formal

Pengendalian formal mencakup mendefinisikan perilaku, mendokumentasikan prosedur dan praktik yang diharapkan, serta mengelola dan mencegah perilaku yang menyimpang dari kebijakan yang berlaku. Kontrol ini bersifat formal karena administrator menghabiskan banyak waktu untuk mempersiapkan dan mendokumentasikannya dan diharapkan efektif dalam jangka panjang.

5) Pengendalian Informal

Pengendalian informal meliputi program pendidikan dan pelatihan serta program pengembangan manajemen. Kontrol ini dirancang untuk memastikan bahwa karyawan perusahaan memahami dan mendukung program keamanan ini.

KESIMPULAN

Dapat disimpulkan bahwa Keamanan liputan (information security) dipakai buat menggambarkan proteksi baik alat-alat computer & non personal komputer & non komputer, fasilitas, data, & liputan menurut penyalahgunaan pihak-pihak yg nir berwenang. Keamanan liputan ditujukan buat mencapai 3 tujuan primer yaitu: kerahasiaan, ketersediaan, & integritas.

Ancaman keamanan sistem informasi, di sisi lain adalah individu, organisasi, mekanisme, atau peristiwa yang dapat merusak aset informasi organisasi. Ancaman terdiri dari ancaman internal dan eksternal. Risiko keamanan informasi didefinisikan sebagai potensi konsekuensi tak terduga dari pelanggaran keamanan informasi karena ancaman keamanan informasi. Semua risiko mewakili tindakan penipuan. Untuk mengontrol ancaman dan risiko keamanan informasi, dapat diimplementasikan dengan berbagai kontrol: teknis, kriptografi, fisik, formal, dan informal.

SARAN

Di dunia sekarang ini, penting untuk melindungi informasi dan sumber daya virtual atau fisik dari ancaman. Kami mendorong organisasi dan komunitas secara keseluruhan untuk memperkuat sistem keamanan mereka dan mencadangkan data penting untuk melindungi data dan informasi mereka. Oleh karena itu, bahkan jika terjadi kesalahan, data yang telah dicadangkan dengan aman tetap ada.

DAFTAR PUSTAKA

- 14 Pengertian Sistem Informasi Manajemen Menurut Ahli - Materi Dosen.* (n.d.). Retrieved January 22, 2022, from <https://www.materidosen.com/2017/04/14-pengertian-sistem-informasi.html>
- Ajie, M. D. (1375). *Sistem Informasi- Konsep Dasar*.
- Hariyanto, S. (2016). Sistem Informasi Manajemen. In *Sistem Informasi Manajemen* (Vol. 9, Issue 1, p. 80). <https://jurnal-unita.org/index.php/publiciana/article/viewFile/75/69>
- Intika, P. D., & Buana, U. M. (2020). *Tugas Sistem Informasi Manajemen : Perkembangan Sistem Pengembangan Sistem Informasi Dosen Pengampu : October*.
- Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008, 2008(semnasIF)*, 379–386.
- Puriwigati, A. N., & Buana, U. M. (2020). *Sistem Informasi Manajemen-Keamanan Informasi. May*.
- Syafrizal, M. (2007). ISO 17799 : Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi 2007 (SNT 2007), 2007(November)*, 1–12.