

PERAN SISTEM INFORMASI AKUNTANSI DALAM PENGAPLIKASIAN ENKRIPSI TERHADAP PENINGKATAN KEAMANAN PERUSAHAAN

Indri Widya Wulandari

Fakultas Ekonomi Dan Bisnis, Universitas 17 Agustus 1945 Surabaya

Email : 1222100151@surel.untag-sby.ac.id

Hwihanus

Fakultas Ekonomi Dan Bisnis, Universitas 17 Agustus 1945 Surabaya

Email: hwihanus@untag-sby.ac.id

Abstract. *An accounting information system (SIA) is a system designed to collect accounting information so that accountants and company executives can make the right decisions. A good system will increase productivity, efficiency, improve customer service, and facilitate decision making. Information security is protecting information from threats that may occur in an effort to ensure business continuity, reduce risk levels and accelerate investment decision making and business opportunities. Companies need to pay attention to the security of their information assets, information leaks and system failures can result in financial losses and company productivity. In this era of rapid growth of information systems, information security is something that must be considered because if information can be monitored by unauthorized or irresponsible people, then the accuracy of the information will be doubted, it will even become misleading information. The use of information technology has tremendous benefits, especially for companies. By using information technology, companies can provide, manage and report finance easily, quickly and accurately. The purpose of information system security is to prevent threats to the system and detect and repair damage that occurs to the system. Threats to information systems are of many kinds, including: data theft, illegal use of the system, illegal destruction of data, illegal modification and failure of the system.*

Keywords: *Accounting Information System, Encry, Information Security.*

Abstrak. Sistem informasi akuntansi (SIA) merupakan sistem yang dirancang untuk mengumpulkan informasi akuntansi sehingga akuntan dan eksekutif perusahaan dapat membuat keputusan yang tepat. Sistem yang baik akan meningkatkan produktifitas, efisiensi, meningkatkan pelayanan pelanggan, dan mempermudah dalam pengambilan keputusan. Keamanan informasi adalah menjaga informasi dari ancaman yang mungkin terjadi dalam upaya menjamin kelangsungan bisnis, mengurangi tingkat risiko dan mempercepat pengambilan keputusan investasi serta peluang bisnis. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian finansial maupun produktifitas perusahaan. Pada era pertumbuhan sistem informasi yang sangat cepat saat ini keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan karena jika sebuah informasi dapat diawasi oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi akan diragukan, bahkan akan menjadi sebuah informasi yang

Received November 30, 2022; Revised Desember 02, 2022; Januari 01, 2023

* Indri Widya Wulandari, 1222100151@surel.untag-sby.ac.id

menyesatkan. Pemanfaatan teknologi informasi memiliki manfaat yang luar biasa, terutama bagi perusahaan. Dengan menggunakan teknologi informasi, perusahaan dapat menyediakan, mengelola, dan melaporkan keuangan dengan mudah, cepat, dan akurat. Tujuan dari keamanan sistem informasi yaitu mencegah ancaman terhadap sistem serta mendeteksi dan memperbaiki kerusakan yang terjadi pada system. Ancaman terhadap sistem informasi banyak macamnya antara lain: pencurian data, penggunaan sistem secara ilegal, menghancurkan data secara ilegal modifikasi secara ilegal dan kegagalan pada sistem.

Kata kunci: System Informasi Akuntansi, Enkripsi, Keamanan Informasi.

LATAR BELAKANG

Di era sistem informasi yang berkembang pesat saat ini, keamanan informasi harus diperhatikan karena informasi dapat berada di bawah kendali orang yang tidak berwenang atau tidak bertanggung jawab, keakuratan informasi dapat diragukan bahkan menjadi informasi yang menyesatkan. Informasi telah menjadi komoditas yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada dalam "masyarakat informasi". Kemampuan untuk menerima dan memberikan informasi dengan cepat dan akurat merupakan hal yang sangat penting bagi setiap organisasi, baik itu organisasi bisnis (perusahaan), universitas, instansi pemerintah, maupun perorangan (pribadi).

Pengamanan data sangat diperlukan, baik data pribadi maupun data perusahaan, Anda harus benar-benar mempercayainya. Perlindungan data membutuhkan kemampuan untuk mencegah penyalahgunaan data. Semua informasi mengandung informasi berharga yang harus dijaga kerahasiaannya. Proses enkripsi adalah proses perlindungan data. Tujuan dari proses enkripsi adalah untuk mengubah data menjadi informasi yang tidak dapat dipahami atau ciphertext

Tingkat keamanan data juga bergantung pada sensitivitas data dalam database, untuk data yang tidak terlalu sensitif, sistem keamanannya tidak terlalu ketat, sedangkan untuk data yang sangat sensitif, harus ditetapkan tingkat keamanan yang ketat untuk mengaksesnya. . data (nasional, 2013). Keamanan informasi merupakan salah satu aspek terpenting dari sebuah sistem informasi. Sayangnya masalah keamanan informasi seringkali kurang mendapat perhatian dari pemilik dan pengelola sistem informasi. Jika mengganggu pengoperasian sistem, keamanan sering kali dilemahkan atau dihilangkan.

Keamanan sistem informasi dibangun oleh banyak kelompok analisis dan pengembang pada saat itu, namun akhirnya ditinggalkan oleh para pengguna. Hal ini

dikarenakan sistem yang dibangun lebih berorientasi pada membuat sistem yang digunakan sulit atau kurang cerdas bagi pengguna, sistem kurang interaktif dan tidak memberikan rasa nyaman kepada pengguna, ketidaksamaan sistem memaksa pengguna untuk mengikuti prosedur yang ada. . dibangun untuk melakukan ini agar sistem terasa nyaman kaku dan kurang dinamis, keamanan sistem informasi yang dibangun tidak terjamin.

Tumbuhnya kesadaran akan pentingnya pengendalian sistem informasi dalam manajemen perusahaan turut memberikan andil dalam hal ini. Meskipun keamanan komputer mengacu pada keamanan informasi yang diterapkan pada komputer dan jaringannya, tujuannya adalah untuk mencegah penipuan dalam sistem data. Keamanan data harus melindungi dari pencurian data dan menjaga kegunaan. Informasi telah menjadi komoditas yang sangat penting. Kemampuan untuk menerima dan memberikan informasi dengan cepat dan akurat merupakan hal yang penting bagi setiap organisasi, baik itu organisasi bisnis (perusahaan), universitas, instansi pemerintah maupun perorangan. Hal ini dimungkinkan oleh pesatnya perkembangan di bidang teknologi informasi dan telekomunikasi.

Dari poin-poin di atas dapat disimpulkan bahwa dalam membangun sebuah sistem informasi, keamanan harus berlandaskan perspektif, sehingga pengguna tidak menghambat atau bahkan mempersulit proses transaksi dan klarifikasi dalam pengambilan keputusan.

KAJIAN TEORITIS

A. Keamanan System Informasi

Menurut Hall (2011), keamanan informasi adalah upaya untuk menghindari kejadian yang tidak diinginkan seperti hilangnya kerahasiaan atau integritas data. Sistem keamanan dimaksudkan untuk mencegah penipuan dan penyalahgunaan sistem komputer lainnya.

Bodnar (2000) menyatakan hal yang sama dengan menyatakan: “Sistem keamanan komputer adalah subsistem dari suatu organisasi yang mengelola risiko spesifik yang terkait dengan sistem informasi terkomputerisasi. Basis Data, Prosedur, dan Laporan Komputer adalah contoh perangkat keras. Sistem keamanan informasi tidak hanya mencakup keamanan fisik, tetapi juga mencakup keamanan non fisik.

Berdasarkan beberapa definisi di atas, dapat disimpulkan bahwa sistem keamanan informasi (komputer) adalah upaya untuk menghindari kejadian yang tidak diinginkan atau risiko tertentu yang berkaitan dengan sistem informasi dan komponennya seperti kehilangan data, kerahasiaan atau integritas data. Keamanan data mengacu pada tindakan privasi digital yang mencegah akses tidak sah ke komputer, database, dan situs web. Keamanan data juga melindungi data dari korupsi. Keamanan data adalah bagian penting dari TI untuk semua ukuran dan jenis bisnis. Keamanan data juga dikenal sebagai keamanan informasi atau keamanan komputer.

B. Pentingnya Keamanan Data

Semua perusahaan saat ini memproses data sampai batas tertentu. Dari bank yang memproses data pribadi dan keuangan dalam jumlah besar hingga bisnis satu orang yang menyimpan informasi kontak pelanggan di ponsel mereka, data penting bagi bisnis besar dan kecil.

Tujuan utama keamanan data adalah untuk melindungi informasi yang dikumpulkan, disimpan, diterima, atau dikirim oleh organisasi. Kepatuhan juga merupakan pertimbangan penting. Apa pun perangkat, teknologi, atau proses yang digunakan untuk mengelola, menyimpan, atau mengumpulkan data, itu harus dilindungi.

C. System Informasi

Sistem informasi, seperangkat komponen terintegrasi yang digunakan untuk mengumpulkan, menyimpan, dan memproses informasi serta menyediakan informasi, pengetahuan, dan produk digital. Bisnis dan organisasi lain mengandalkan sistem informasi untuk mengelola dan mengendalikan operasi mereka, berkomunikasi dengan pelanggan dan pemasok mereka, dan bersaing di pasar. Sistem informasi digunakan untuk mengelola rantai pasokan antara organisasi dan pameran elektronik. Semua orang mengandalkan sistem informasi, biasanya Internet, untuk sebagian besar kehidupan pribadi mereka.

D. Sistem Informasi Akuntansi

Sistem informasi akuntansi mengumpulkan, menangkap, menyimpan, dan memproses akuntansi dan data untuk menciptakan informasi bagi para pengambil keputusan (Romney dan Steinbart, 2016:11). Pendapat lain mengatakan bahwa sistem akuntansi adalah suatu organisasi formulir, catatan dan laporan yang dikoordinasikan sebagai penyedia informasi keuangan untuk memudahkan manajemen dalam tata kelola

perusahaan (Mulyadi, 2016:3). Sistem informasi akuntansi mencakup proses, prosedur, dan sistem yang mengumpulkan informasi akuntansi tentang proses bisnis, menyimpan informasi akuntansi dalam catatan yang sesuai, memproses informasi akuntansi secara terperinci melalui klasifikasi, agregasi, dan agregasi, serta melaporkan ringkasan informasi akuntansi kepada pengguna internal dan eksternal.

E. Bagian Bagian System Informasi Akunrtansi

Terdapat beberapa bagian krusial pada sistem liputan akuntansi. Bagian tadi meliputi:

1. People yg bertugas mengoperasikan sistem dan melakukan ragam fungsi.
2. Procedure yakni bagian yg mengumpulkan, memproses, dan menyimpan data yg terdapat hubungannya menggunakan kegiatan organisasi.
3. Data yakni bagian yg melakukan aktivitas & proses bisnis.
4. Software adalah bagian yg memproses data yg masih ada dalam organisasi.
5. Infrastruktur Informasi Teknologi yg terdiri menurut personal komputer dan alat-alat lain.

F. Penerapan Sistem Informasi Akuntansi

Penerapan sistem adalah proses menginstal sistem baru yang mencakup semua perangkat keras dan perangkat lunak yang dibeli. Sedangkan implementasi sistem informasi akuntansi adalah pelaksanaan berbagai aktivitas akuntansi untuk menghasilkan informasi komputer yang relevan, tepat waktu, andal, dan dapat dipercaya (Rafflis, 2012). Menurut Nugroho (2011), dalam Rafflis (2012), tujuan penerapan sistem informasi akuntansi dapat disimpulkan sebagai berikut: (1) Memberikan informasi tagihan yang cepat (2) Menciptakan informasi tagihan yang efisien (3) Membuat informasi tagihan yang dapat dipercaya (4) Membuat informasi tagihan yang berguna untuk perencanaan.

G. Efektivitas Penggunaan Sistem Informasi Akuntansi

Efisiensi mengukur seberapa baik pekerjaan dapat dilakukan dan sejauh mana seseorang dapat mencapai hasil yang diharapkan (Kristiani, 2012 dalam Astuti 2014). Suatu sistem dapat dikatakan efektif bila dapat menghasilkan informasi yang dapat diterima dan memenuhi harapan informasi secara tepat waktu, akurat dan dapat diandalkan (Widjajanto, 2001 dalam Ratnaningsih, 2014). Deghazade et al. (2011), efisiensi data sistem akuntansi terkomputerisasi memiliki beberapa kriteria, antara lain:

- a. Melengkapi informasi yang diharapkan pengguna dari sistem (termasuk administrasi).

- b. Pertimbangkan kewajiban hukum
- c. Mampu memberikan laporan keuangan kepada pihak internal dan eksternal

Menurut DeLone dan McClean (1992), sistem informasi akuntansi dapat dikatakan efisien. Pratama (2013) harus memenuhi persyaratan berikut: Informasi yang dihasilkan harus berkualitas tinggi dan terkait dengan hasil sistem informasi. Novita (2011) dalam Pratama (2013) menyatakan bahwa semakin efektif sistem informasi akuntansi akan meningkatkan kinerja pegawai.

H. Enkripsi

Enkripsi adalah aktivitas mengubah bentuk data yang awalnya mudah dipahami menjadi kode yang sulit dipahami. Hal tersebut karena fungsi utama enkripsi adalah mengamankan data. Enkripsi dipakai untuk menanggulangi seiring adanya cyber crime atau (kejahatan dunia maya). Seperti peretasan email, phishing, pencurian data, carding, dan sejenisnya.

Caranya, dengan mengacak data sensitif agar berbeda dengan aslinya. Dengan begitu, ketika hacker menerima data, mereka tidak bisa dengan mudah menggunakannya. Itu mengapa, berbagai platform digital seperti situs web dan media sosial kini memakai enkripsi.

Enkripsi dibuat untuk mengamankan atau merahasiakan data. Data yang terenkripsi masih bisa didekripsi alias diubah menjadi teks seperti asalnya. Dengan catatan, seseorang memang memiliki hak akses atau merupakan pemilik akun yang sah.

METODE PENELITIAN

Enkripsi adalah kontrol preventif yang dapat digunakan untuk melindungi dan menjaga kerahasiaan. Metode yang digunakan untuk menulis artikel ini menggunakan metode penelitian kepustakaan atau literature research. Tinjauan pustaka dilakukan dengan cara mengumpulkan referensi yang terdiri dari beberapa penelitian terdahulu kemudian menggabungkannya menjadi sebuah kesimpulan (Mardalis, 1999). Kajian sastra dapat diperoleh dari berbagai sumber seperti surat kabar, buku, dokumen, internet dan perpustakaan. Metode penelitian kepustakaan merupakan rangkaian kegiatan yang berkaitan dengan metode pengumpulan data pustaka, membaca dan mencatat, serta pengelolaan makalah (Zed, 2008 Nursalam, 2016). Berdasarkan referensi yang diterima,

kami memutuskan 1.) Apa peran penting sistem informasi akuntansi di perusahaan? 2.) Faktor apa yang mempengaruhi kekuatan enkripsi?

Walaupun terlihat sederhana, kajian literatur membutuhkan banyak tekad agar data dan analisis data serta kesimpulan yang dihasilkan sesuai dengan tujuan yang diharapkan. Ini membutuhkan persiapan dan pelaksanaan yang optimal. Mempelajari literatur membutuhkan analisis yang matang dan menyeluruh untuk membuahkan hasil dan tidak ada privasi. Enkripsi melindungi data saat bergerak melalui Internet dan juga merupakan penghalang terakhir yang harus dilalui penyusup untuk mendapatkan akses tidak sah ke data yang disimpan. Enkripsi adalah proses mengubah teks normal, yang disebut plaintext, menjadi ciphertext yang tidak dapat dibaca, yang disebut ciphertext.

HASIL DAN PEMBAHASAN

Enkripsi adalah kontrol pencegahan yang dapat digunakan untuk melindungi kerahasiaan dan privasi. Enkripsi melindungi data saat bergerak melalui Internet dan juga merupakan penghalang terakhir yang harus dilalui penyusup untuk mendapatkan akses tidak sah ke data yang disimpan. Enkripsi adalah proses mengubah teks normal, yang disebut plaintext, menjadi ciphertext yang tidak dapat dibaca, yang disebut ciphertext.

Faktor faktor yang mempengaruhi kekuatan enkripsi:

1. Panjang kunci

Kunci yang lebih panjang memberikan enkripsi yang lebih kuat dengan mengurangi jumlah balok-balok yang berulang pada ciphertext. Hal tersebut menjadikan lebih sulit untuk menunjukkan pola pola ciphertext yang merefleksikan pola –pola plaintext asli. Dalam bahas inggris, 8 bit mempresentasikan masing – masing huruf. Hal ini mempermudah penggunaan informasi terkait frekuensi kata yang relatif. Itulan menggapa sebagian besar kunci enkripsi setidaknya sepanjang 256 bit (setara denga 42 huruf Bahasa inggris.), dan seringnya adalah 1.024 bit atau panjang lagi

2. Alogaritme enkripsi

Jenis yang digunakan untuk menghubungkan kunci ke plaintext sangat penting. Algoritme yang kompleks dan kuat yang bukan tidak mungkin diretas menggunakan teknik brute force. Kerahasiaan tidak diperlukan untuk kekuatan. Kekuatannya tidak terletak pada kerahasiaan operasinya, tetapi pada kenyataan

bahwa algoritme tersebut telah diuji secara ketat dan terbukti tahan terhadap serangan taruhan brute force.

3. Kebijakan untuk mengelola kunci kriptografi

Manajemen kunci kriptografi sering kali merupakan aspek yang paling rentan dari sistem enkripsi. Penting juga untuk mengembalikan kunci dengan cepat jika karyawan berhenti bekerja atau jika ada alasan untuk meyakini bahwa kunci telah disusupi dan untuk memberi tahu mereka yang mempercayai kunci bahwa kunci tersebut salah.

Jenis Jenis System Enkripsi

Pada sistem ini ada dua jenis dasar dalam sistem enkripsi, yaitu :

1. System enkripsi simetris (*symmetric encryption system*)

Menggunakan kunci yang sama untuk mengenkripsi. DES dan AES adalah contoh dari sistem enkripsi simetris

2. System enkripsi asimetris (*asymmetric encryption system*)

Menggunakan dua kunci. Satu kunci disebut kunci publik (*public key*), didistribusikan secara luas dan tersedia untuk siapapun, kunci lainnya disebut dengan kunci privat (*private key*), dirahasiakan dan diketahui hanya publik dari sepasang kunci tersebut. Baik kunci publik dan privat dapat digunakan untuk mengenkripsi, tetapi hanya satu kunci yang dapat mendiskripsi *chiphertext*. RSA dan PGP merupakan contoh dari sistem enkripsi asimetris.

	Enkripsi Simetris	Enkripsi Asimetris
Jumlah Kunci	Satu kunci Kunci rahasia yang di gunakan baik untuk mengenkripsi maupun deskripsi adalah sama.	Dua kunci Satu kunci bersifat publik, yang lainnya pribadi. Kedua kunci dapat mengenkripsi, tetapi hanya satu kunci yang dapat mendekripsi
Keunggulan	<ul style="list-style-type: none"> • Kecepatan jauh lebih cepat 	<ul style="list-style-type: none"> • Siapa pun dapat menggunakan kunci publik Anda untuk berkomunikasi dengan Anda • Tidak perlu menyimpan kunci untuk setiap pihak yang ingin Anda ajak berkomunikasi • Dapat digunakan untuk membuat tanda tangan digital yang sah
Kekurangan	<ul style="list-style-type: none"> • Memerlukan kunci terpisah bagi siapapun yang ingin berkomunikasi • Cara yang aman harus ditemukan untuk berbagi kunci rahasia dengan pihak lain. 	<ul style="list-style-type: none"> • Kecepatan jauh lebih lambat • Memerlukan PKI untuk memvalidasi kepemilikan kunci public
Isu – Isu Resiko	<ul style="list-style-type: none"> • Melindungi kunci rahasia bersama dari kehilangan atau pencurian 	<ul style="list-style-type: none"> • Melindungi kunci privat dari kehilangan atau pencurian
Penggunaan Utama	<ul style="list-style-type: none"> • Enkripsi untuk data dalam jumlah besar 	<ul style="list-style-type: none"> • Pembuatan tanda tangan digital • Pertukaran keamanan atas kunci simetris melalui e-mail.

Diatas Table Perbandingan System Enkripsi Simetris Dan Asimetris

Pada dua jenis system enkripsi, hilang atau dicurinya kunci enkripsi merupakan ancaman besar. Jika kunci ini hilang, informasi yang dienkripsi tidak dapat dipulihkan. Salah satu solusi untuk ancaman ini adalah menggunakan perangkat lunak enkripsi yang menciptakan sebuah kunci utama *built-in* yang dapat digunakan untuk mendiskripsi apa saja yang di enkripsi oleh perangkat lunak tersebut. Alternatifnya adalah sebuah proses yang disebut **key escrow**, proses yang melibatkan pembuatan salinan dari seluruh kunci enkripsi yang digunakan oleh para pegawai dan menyiapkan salinan tersebut dengan aman.

Dalam system simetris, jika kunci rahasia yang dibagikan telah dicuri, penyerang dapat mengakses segala informasi yang dienkripsi olehnya. Dalam system asimetris, kunci public dimaksudkan untuk mendistribusikan secara luas, tetapi kunci privat harus disimpan dengan aman. Enkripsi simetris jauh lebih cepat daripada enkripsi asimetris, tetapi ia memiliki dua masalah besar. E-mail bukanlah sebuah solusi, karena siapapun yang dapat memotong e-mail akan mengetahui kunci rahasianya. Oleh Karena itu, beberapa metode pertukaran kunci dengan sarana lain diperlukan.

Contoh penggunaan enkripsi

1. Penggunaan SSL

SSL ada contoh enkripsi yang dipakai pada website. Ciri website yang memakai enkripsi SSL adalah terdapat logo gembok atau awalan https. Bisa dikatakan, cara meningkatkan keamanan website memang dengan memasang SSL.

2. Penggunaan SSH

SSH adalah singkatan dari Secure Shell Connection. SSH biasanya digunakan untuk mengakses, mengontrol, dan mengelola server secara remote melalui internet. Karena pastinya berkaitan dengan data sensitif, SSH ini memakai enkripsi untuk memastikan kerahasiaan dan keutuhan data antara client dan server.

3. E2EE

E2EE adalah singkatan dari enkripsi end to end. Biasanya dipakai aplikasi chat. Jangan salah, pesan yang sedang dikirim juga bisa bocor ke pihak ketiga. Oleh karena itu, pesan perlu dienkripsi agar tidak bocor. Namun, enkripsi E2EE merupakan enkripsi user to user. Sehingga datanya kemungkinan masih bisa dilihat oleh pihak service provider.

Kekurangan utama dari sistem enkripsi asimetris adalah kecepatannya. Enkripsi asimetris jauh lebih lambat daripada enkripsi simetris, membuatnya tidak praktis untuk digunakan dalam pertukaran jumlah data yang lebih besar melalui internet. Akibatnya, e-bisnis menggunakan kedua jenis sistem enkripsi. Prediksi simetri digunakan untuk menyanding atau encode sebagian besar data yang dipertukarkan, sedangkan enkripsi asimetris digunakan untuk mengirim kunci simetris secara aman melalui email pada penerima agar digunakan untuk mendeskripsi ciphertext. Kunci rahasia yang dibagikan tersebut aman, bahkan jika dikirim melalui email karena apabila pengiriman menggunakan kunci publik penerima untuk menenkripsinya, maka hanya penerima yang dikehendaki yang menjadi satu-satunya pemilik kunci privat terkait dan dapat mendeskripsikan kunci simetris rahasia yang dibagikan tersebut.

Bahwa setiap perusahaan atau organisasi pasti memiliki data sensitif atau rahasia, sehingga perusahaan harus mengambil langkah-langkah untuk meningkatkan keamanan data. beberapa cara untuk melakukan ini membangun keamanan informasi di perusahaan Anda, antara lain:

- 1. Membuat Kebijakan Untuk Menangani Segala Macam Informasi**

Sebuah organisasi tidak dapat membedakan dengan benar antara informasi rahasia dan non-rahasia, menjadi sulit untuk melindungi informasi bisnis yang penting. Oleh karena itu, kebijakan data diperlukan untuk menjelaskan data sensitif dan untuk dapat menentukan proses yang ketat untuk mengidentifikasi, menangani, dan melindungi berbagai jenis data.

- 2. Menggunakan Enkripsi Untuk Mentransfer Data**

Banyak organisasi telah menyadari pentingnya menerapkan langkah-langkah keamanan informasi untuk melindungi data dalam sistem informasi dan jaringan perusahaan terhadap akses yang tidak sah. Semua jenis orang dan aplikasi selalu mengakses dan berinteraksi dengan data sensitif. Oleh karena itu, melindungi data saat digunakan di seluruh sistem mengharuskan organisasi mengenkripsi data yang berguna untuk melindungi dan mengamankan data itu sendiri.

3. Memilih *Software* yang Aman Untuk Organisasi

Cari tahu perangkat lunak mana yang direkomendasikan oleh pakar keamanan informasi untuk standar keamanan yang digunakan. Perangkat lunak yang Anda gunakan mungkin tidak mengikuti metode keamanan yang andal dan dapat meningkatkan kemungkinan *heacker* mendapatkan akses ke informasi sensitif.

4. Meningkatkan Keamanan *Password*

Menggunakan kata sandi atau kata sandi yang lemah adalah masalah yang sangat umum, keamanannya dapat ditingkatkan secara signifikan melalui pelatihan dan pengenalan berbagai aplikasi manajemen kata sandi. Sebagian besar pencurian data sensitif disebabkan oleh beberapa kesalahan keamanan dasar.

5. Menerapkan Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi, singkatnya ISO/IEC 27001, adalah metode terstruktur khusus untuk melindungi informasi yang diakui secara internasional. ISO/IEC 27001 adalah dokumen Sistem Manajemen Keamanan Informasi yang memberikan gambaran tentang apa yang harus dilakukan perusahaan atau organisasi untuk menilai, menerapkan, dan memelihara keamanan informasi berdasarkan praktik terbaik keamanan informasi.

Penerapan beberapa metode ini akan mengamankan aset informasi dan melindunginya dari ancaman pihak tidak berwenang yang menggunakan informasi tersebut untuk keuntungan yang merugikan organisasi atau bisnis.

Informasi adalah sumber daya yang sangat berharga bagi individu, otoritas dan sektor swasta. Informasi memiliki nilai dan harus dilindungi, sehingga penting bagi individu untuk melindungi informasi. Informasi sangat berharga karena jika berada di tangan pihak yang tidak bertanggung jawab dapat disalahgunakan.

Dalam memanfaatkan teknologi informasi yang luar biasa besar, terutama bagi perusahaan. Dengan menggunakan teknologi informasi, perusahaan dapat menyediakan, mengelola, dan melaporkan keuangan dengan mudah, cepat, dan akurat. Dalam akuntansi, pasti mengenal Sistem Informasi Akuntansi (SIA). Peran sistem informasi akuntansi dalam perusahaan. Pemanfaatan teknologi informasi memiliki manfaat yang luar biasa besar, terutama bagi perusahaan.

Dari data yang dimasukkan oleh orang tersebut dilakukan pengolahan data sesuai dengan prosedur yang berlaku, sehingga hasilnya berupa data akuntansi. Agar hasil data akuntansi akurat, mutakhir dan bermanfaat bagi pengguna, maka seluruh bagian SIA harus terintegrasi dengan baik dan benar.

Manfaat memiliki sistem informasi akuntansi untuk bisnis adalah beberapa hal yang perlu diketahui:

- a. Memberikan informasi yang akurat dan ringkas dengan cara yang berdampak pada perkembangan perusahaan.
- b. Meningkatkan efisiensi dalam perusahaan sehingga menghasilkan peningkatan pendapatan.
- c. Mari tingkatkan kemampuan perusahaan untuk mengambil keputusan yang cerdas.
- d. Meningkatkan berbagi informasi perusahaan.
- e. Meningkatkan efisiensi kerja di departemen keuangan perusahaan berkat sistem informasi akuntansi.
- f. Untuk meningkatkan kualitas produk yang diproduksi. Pengurangan biaya produksi dan jasa dalam proses produksi produk perusahaan.

Berdasarkan penjelasan di atas, sistem informasi akuntansi memegang peranan penting dalam kemajuan perusahaan. SIA memainkan banyak peran penting dalam perusahaan, seperti: Meningkatkan kualitas dan mengurangi biaya dalam produksi barang dan jasa, meningkatkan pengambilan keputusan, dan menciptakan keunggulan kompetitif. Diantara sekian banyak fungsi SIA, terdapat 3 fungsi utama yang dibentuk SIA dalam perusahaan. Selain pengambilan keputusan, ini juga mencakup pengumpulan dan penyimpanan data peristiwa, pemrosesan data menjadi informasi yang dapat ditindaklanjuti, dan pengelolaan aset perusahaan.

Dengan SIA yang baik, organisasi dapat mengoperasikan proses operasional dan informasi dengan lebih efisien dan efektif, karena proses tersebut diatur oleh kontrol sedemikian rupa sehingga hasil yang dicapai dapat diselaraskan dengan tujuan organisasi. Selain itu, data akuntansi yang dihasilkan oleh SIA dapat dipertimbangkan untuk digunakan nanti dalam pengambilan keputusan tentang keuangan perusahaan, maupun untuk digunakan oleh pihak di luar perusahaan seperti pemasok, investor, dan pelanggan yang terkait langsung dengan bisnis perusahaan.

Jika SIA dalam suatu perusahaan tidak berjalan dengan baik, misalnya karena beberapa komponen SIA tidak bekerja secara maksimal, tentu akan mempersulit sistem sehingga bisnis perusahaan tidak berjalan dengan sempurna. , informasi yang dihasilkan tidak benar dan tujuan bisnis perusahaan sulit dicapai. Oleh karena itu, perusahaan harus merancang dan mengimplementasikan SIA terbaik untuk kelancaran operasi bisnis dan pencapaian tujuan perusahaan. Selain SIA, sistem informasi lainnya harus dirancang dan diimplementasikan sebaik mungkin agar bisnis perusahaan dapat berjalan dengan efisien dan efektif serta perusahaan dapat berkembang dari waktu ke waktu.

Tidak hanya itu, dalam menjalankan perusahaan Anda juga perlu melakukan administrasi keuangan yang baik, SIA di kombinasikan dengan administrasi keuangan yang baik pastinya akan menghasilkan hasil yang lebih baik.

KESIMPULAN

Enkripsi melindungi data saat bergerak melalui Internet dan juga merupakan penghalang terakhir yang harus dilalui penyusup untuk mendapatkan akses tidak sah ke data yang disimpan. Tujuan dari proses enkripsi adalah mengubah data menjadi informasi atau ciphertext yang tidak dapat dipahami. Tingkat keamanan data juga tergantung pada sensitivitas data dalam database, untuk data yang tidak terlalu sensitif sistem keamanannya tidak terlalu ketat, sedangkan untuk data yang sangat sensitif perlu diatur tingkat keamanan yang lebih tinggi.

SIA memainkan banyak peran penting dalam perusahaan, seperti: Meningkatkan kualitas dan mengurangi biaya dalam produksi barang dan jasa, meningkatkan pengambilan keputusan, dan menciptakan keunggulan kompetitif. Dengan bantuan SIA, perusahaan dapat melakukan segala aktivitasnya dengan lebih efektif dan efisien. Selain itu, manajemen keuangan yang baik juga diperlukan untuk menjalankan bisnis, SIA yang dikombinasikan dengan manajemen keuangan yang baik pasti akan memberikan hasil yang lebih baik.

DAFTAR REFERENSI

- Aqham, A. A. (2022, Januari 11). *Peran Sistem Informasi Akuntansi dalam Perusahaan*. Retrieved from <http://komputerisasi-akuntansi-d4.stekom.ac.id: http://komputerisasi-akuntansi-d4.stekom.ac.id/informasi/baca/Peran-Sistem-Informasi-Akuntansi-Dalam-Perusahaan/da7326f9191a38242070253a03a371ca4b654/informasi/baca/Peran-Sistem-Informasi-Akuntansi-Dalam-Perusahaan/da7326f9191a38242070253a03a371ca4b65452d>
- Awinda, S. (2019). *Perancangan Aplikasi Enkripsi dan Deskripsi dengan Teknik Transposisi Baris dan Kolom*. Retrieved from <https://journal.pancabudi.ac.id: https://journal.pancabudi.ac.id/index.php/fastek/article/download/1749/1590>
- Lusianah, S. M. (2020, Desember 17). *Keamanan Komputer Dan Sistem Informasi Akuntansi*. Retrieved from <https://accounting.binus.ac.id: https://accounting.binus.ac.id/2020/12/17/keamanan-komputer-dan-sistem-informasi-akuntansi/>
- Marsiani. (2021). *JRKT (Jurnal Rekayasa Komputasi Terapan)*. Retrieved from <http://jim.unindra.ac.id: http://jim.unindra.ac.id/index.php/JRKT/article/view/4096/492>
- Mengamankan Informasi Perusahaan*. (2021, Februari 08). Retrieved from <https://isokonsultindo.com: https://isokonsultindo.com/cara-mengamankan-informasi-perusahaan.php>
- Paryati. (2008, Mei 24). *Keamanan Sistem Informasi*. Retrieved from <https://media.neliti.com: https://media.neliti.com/media/publications/174555-ID-keamanan-sistem-informasi.pdf>
- Sistem Informasi Akuntansi: Pengertian, Fungsi, Contoh*. (n.d.). Retrieved from <https://www.jurnal.id: https://www.jurnal.id/id/blog/pengertian-dan-fungsi-sistem-informasi-akuntansi-dalam-perusahaan/>
- Marshall B. Roomney, P. J. (2019). *Sistem Informasi Akuntansi Edisi 13*. Jakarta Selatan: Penerbit Salemba Empat.