Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Perakitan Elektronik

Zulkarnain, S. Kom., MMSI
Dosen Sistem Informasi
Email : zulbtm@gmail.com

Abstract

Penelitian ini bertujuan untuk menganalisis program keamanan sistem informasi pada sebuah perusahaan perakitan elektronika. Pengolahan data merupakan bagian dari operasional bisnis perusahaan. Kerahasiaan, integritas dan ketersediaan informasi menjadi salah satu fokus perusahaan. Dengan menggunakan metode penelitian deskriptif, dimana penulis menggambarkan dan mendeskripsikan fakta yang terjadi atau program apa saja yagn dilakukan berkaitan dengan keamanan sistem informasi. Penulis akan melakukan pengamatan dan pengecekan secara langsung. Hasil dari penelitian akan dapat mengungkapkan sejauh mana program atau aktifitas yang dilakukan dan mengetahui tingkat keberhasilan dari program atau aktifitas yang dijalankan. Dengan mengetahui keberhasilan dalam menjalankan program ini, maka perusahaan akan merasa tenang bahwa informasi perusahaan dapat terkontrol, dilindungi serta dapat diakses ketika diperlukan. Selain itu juga penelitian ini bisa dijadikan perusahaan lain sebagai referensi untuk menerapkan keamanan sistem informasi. Sehingga keberlangsungan bisnis perusahaan dapat terus berjalan.

***Keywords**: Keamanan sistem informasi, penelitian deskiptif*

I. INTRODUCTION

Persaingan bisnis pada industri perakitan elektronika semakin tinggi. Setiap perusahaan berusaha melakukan penelitian untuk menciptakan produk terbaru mereka yang dapat diterima pasar. Perkembangan teknologi begitu cepat dan memberikan banyak manfaat buat kehidupan manusia. Perkembangan teknologi sangat bervariasi, baik untuk kebutuhan telekomunkasi seperti handphone, dengan beragam fitur dan kemudahaan yang diberikan kepada pengguna. Dalam dunia otomotif juga tidak ketinggalan perkembangannya, bermacam model mobil yang terus dipasarkan dalam dunia otomotif. Semua perkembangan teknologi ini didukung oleh penelitian, dengan memerlukan modal yang besar serta membutuhkan waktu yang panjang. Maka dengan ini, seluruh hasil penelitian dan penemuan perusahaan harus dijaga agar tidak dicuri atau diketahui oleh pihak lain atau pihak kompetisi, dengan tujuan agar perusahaan dapat terus bersaing dalam kompetisi bisnis.

Keamanan informasi merupakah konsep untuk mengamankan asset informasi perusahaan terhadap berbagai ancaman yang dapat memberikan dampak pada perusahaan tersebut (Sarno dan Iffano, 2010).

Ada beberapa elemen dasar yang berkaitan dengan keamanaan informasi seperti kerahasiaan, integritas and juga ketersedian yang merupakan dasar dari program keamanan informasi yang terus dilakukan pengembangan. Ketiga elemen tersebut merupakan konsep yang saling terhubung satu dengan lainnya atau menjadi mata rantai yang saling berhubungan satu dengan lainnya.

Dalam hal ini, penulis melakukan penelitian pada salah satu perusahaan perakitan elektronika untuk mengetahui sejauh mana program yang dilakukan saat ini bermanfaat terhadap keamanan sistem informasi di perusahaan tersebut.

Rumusan Masalah yang akan menjadi arah penelitian ini adalah sebagai berikut:

1. Bagaimana mengetahui tingkat kesadaran karyawan terhadap pentingnya keamanan informasi?
2. Bagaimana mengetahui tingkat kualitas sebuah informasi?
3. Apakah ada infastrutkur yang berkaitan dengan menjaga keamanan informasi?

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui dan mengambil langkah penting untuk meningkatkan kesadaran pentingnya keamanan informasi
2. Membuat klasifikasi terhadap informasi yang ada di perusahaan
3. Mengetahui dan meningkatkan keamanan informasi dengan dukungan infrastuktur

II. LANDASAN TEORI

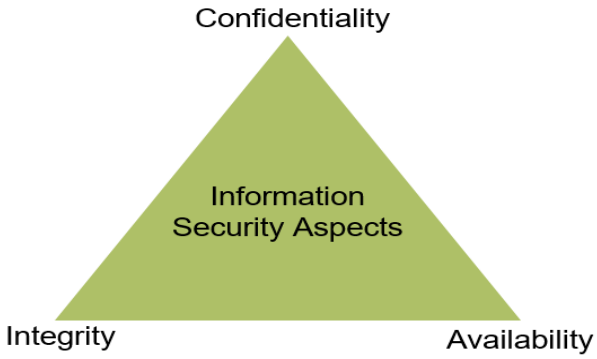
Keamanan sistem informasi merupakan suatu hal penting yang menjadi perhatian khusus bagi perusahaan untuk menjaga agar seluruh informasi yang ada diperusahaan dapat terkontrol dengan baik. Sistem informasi adalah kumpulan dari komponen yagn saling berhubungan satu diantara lainnya, dikumpulkan, diproses, disimpan dan didistribusikn untuk menunjang perusahaan dalam mendapatkan keputusan yang terbaik bagi perusahaan (Kenneth dan Jane, 2007).

Informasi didapatkan dari hasil pengolahan data yang ada dalam suatu organisasi, pengolahan data dilakukan dengan dukungan system.

Pentingnya informasi dalam perusahaan membuat kita harus menjaganya agar selalu dilindungi dan terbebas dari segala macam ancaman. Ancaman bisa datang dari dalam organisasi, seperti tidak adanya evaluasi secara berkala dari system yang berjalan, atau adanya tindakan dari karyawan yang tidak mematuhi aturan organisasi. Ancaman dari luar bisa dalam bentuk penyerangan system dengan tujuan ingin merusak bisnis yang berjalan atau bentuk sabotase lainnya.

Dengan keamanan informasi ini, kita mampu mendeteksi lebih dini kemungkinan serangan terhadap informasi yang dimiliki perusahaan. Dengan mendeteksi secara dini, perusahaan akan mampu mengambil langkah – langkah untuk mencegah serangan atau bahaya yang ditimbulkan. Setiap organisasi mempunyai cara mereka tersendiri untuk mendeteksi masalah yang timbul. Adakalanya cara tersebut didapatkan dari buku, referensi di internet maupun cara yang didapat dari pengalaman.

Ada tiga aspek yang berkaitan dengan keamanan informasi seperti confidentiality, integrity dan availability.



Gambar 1. Keamanan Informasi (Sarno & Iffano, 2009)

Dari gambar diatas ini, dapat kami jelaskan bahwa, Confidentiality adalah kerahasian informasi hanya diakses olah orang tertentu atau pembatasan akses pada informasi yang ada diperusahaan, hanya orang – orang tertentu yang diberikan akses untuk melihat data tersebut. Integrity adalah tingkat akurasi dan kelengkapan dari informasi yang terkontrol, data yang terkontrol adalah data yang terjaga sesuai dengan keinginan kita. Sedangkan availability adalah ketersediaan informasi selalu bisa diakses oleh orang yang telah mendapat izin untuk mengakses data tersebut sesuai dengan kebutuhannya.

Keamanan informasi merupakan suatu yang penting bagi organisasi. Penerapan keamanan informasi menggunakan referensi dari ISO 27001. Dengan standarisasi ini, organisasi akan mendapatkan keamanan dengan level yang berkualitas tinggi.

Perusahaan yang menerapkan standar ISO 27001 akan memberikan manfaat untuk mengendalikan risk pada keamaman informasi dan melindungi kerahasiaan, integritas dan ketersediaan informasi.

Banyak manfaat yang didapat dengan implementasi dari ISO 27001, diantaranya adalah melindungi informasi perusahaan, mengelola risiko keamanan secara efektif dan menjaga citra perusahaan agar bisnis perusahaan dapat berjalan dengan lancar.

III. METODE PENELITIAN

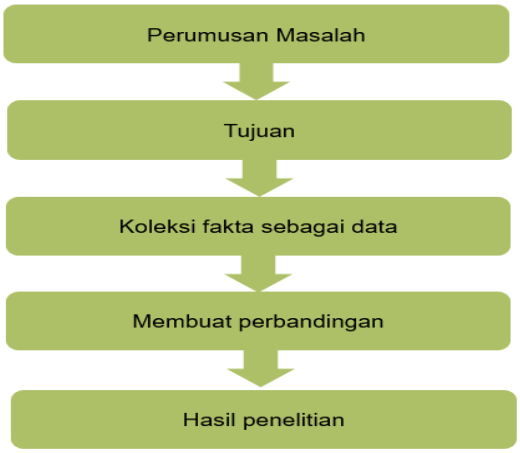
Tujuan dari penelitian ini adalah untuk melakukan evaluasi keamanan informasi perusahaan dan memberikan hasil dari evaluasi kepada perusahaan. Evaluasi ini harus dilalSerta memberikan kebebasan perusahaan untuk mengambil keputusan setelah dilakukan penyajian presentasi keapada perusahaan.

Metode penelitian yang dilakukan adalah dengan menggunakan metode deskrptif.

Menurut Nazir (1988), metode deskriptif adalah suatu metode yang melakukan penelitian berdasarkan suatu objek atau kondisi pada masa sekarang.

Dengan penelitian ini, penulis dapat membuat laporan yang memberikan gambaran secara sistematis dan akurat mengenai fakta yang ada.

Langkah – langkah yang digunakan dalam peneliti dalam melakukan penelitian adalah dengan melakukan langkah sebagai berikut:



Gambar 2. Metode Penelitian

Langkah – langkah yang digunakan dalam penelitian pertama adalah melakukan perumusan masalah yang jelas. Masalah yang diambil harus dilakukan secara spesifik. Kedua menentukan tujuan berdasarkan masalah yang ada. Oraganisasi harus mentukan tujuan yang akan mereka capai. Ketiga adalah menjadikan fakta – fakta sebagai sumber data, data yang diambil sesuai dengan data yang ada dilapangan. Keempat melakukan perbandingan, serta yang kelima adalah hasil penelitian yang telah dilakukan.

IV. HASIL DAN PEMBAHASAN

Dalam bagian ini, saya akan menyampaikan hasil hasil dari pengecekan secara langsung keamanan system informasi pada PT. XYZ. Ada beberapa parameter yang dijadikan sebagai bahan untuk melakukan pengecekan. Paramater ini menjadi dasar bagi penulis untuk melakukan pengecekan pada PT. XYZ. Pengecekan tersebut akan punulis tampilkan dalam bentuk tabel, sehingga penulis dapat mengetahui kondisi perusahaan dengan hasil isian pada tabel tersebut. Dan penulis akan memberikan penilaian sederhana, apakah parameter harus dipertahankan atau masih perlu perbaikan.

Tabel 1. Parameter yang kesadaran karyawan dan adanya pelatihan keamanan informasi

Parameter	Hasil Observasi	Penilaian
Pemahaman karyawan tentang pentingnya keamanaan system informasi pada perusahaan	Karywawan memahami pentingnya keamanan informasi, namun tidak mengetahui secara keseluruhan program yang dijalankan	Perbaikan. Memperkenalkan kembali tentang pentingnya menjaga keamanan informasi
Tingkat kesadaran bagi karyawan untuk melindungi system dari ancaman virus dan malware	Karyawan memahami pentingnya melindungi perusahaan dari bahaya virus, akan tetapi detection virus masih terjadi	Perbaikan. Melakukan presentasi kembali tentang bahaya virus yang dapat merusak sistem
Pelatihan keamanan informasi	Pelatihan telah dilakukan, namun belom seluruh karyawan mendapatkan latihan ini	Perbaikan Melakukan pelatihan secara keseluruhan

Tabel 2. Pengecekan perusahaan dalam menangani informasi penting

Parameter	**Hasil Observasi**	**Penilaian**
Pengecekan klasifikasi informasi penting	Perusahaan melakukan klasifikasi informasi seperti confidential, internal dan public	Pertahankan

Tabel 3. Ketersediaan infrastruktur untuk mendukung keamanan informasi

Parameter	**Hasil Observasi**	**Penilaian**
Adanya penggunaan encrypted untuk informasi yang confidential	Karyawan menggunakan encrypted email untuk komunikasi	Pertahankan. Aplikasi encrypted tersedia

	yang bersifat confidential	
Kontrol akses ruangan penyimpanan data	Setiap ruangan yang mempunyai tingak keamanan informasi yang tinggi dilengkapi dengan hak akses	Pertahankan Menggunakan teknologi Lenel System
Computer khusus untuk membersihkan personal flash disk	Tersedia computer khusus untuk membersihkan personal flash disk sebelum digunakan di computer perusahaan	Pertahankan. Menggunakan computer khusus untuk pengecekan personal flash disk
Aplikasi Inventory untuk mengidentifikasi infrastruktur yang berhubungan dengan keamanan informasi	Tersedia aplikasi inventori, Semua infrastruktur tercatat dalam aplikasi inventory	Pertahankan Menggunakan aplikasi khusus yang dilakukan update secara berkala

V. KESIMPULAN

Dari hasil evaluasi yang dilakukan pada PT. XYZ, berkaitan dengan implementasi keamanan system informasi dengan menggunakan beberapa parameter yang disampaikan pada tabel 1. Kami menyimpulkan sebagai berikut :

1. Perusahaan perlu meningkatkan kesadaran kepada seluruh karyawan tentang pentingnya menjaga keamanan informasi.
2. Adanya klasifikasi informasi secara internal yang bermanfaat untuk melindungi informasi serta kegiatan pencegahan dilakukan secara tepat
3. Perusahaan memiliki infrastruktur yang mendukung kegiatan keamanan informasi. Infrastuktur ini harus terus dirawat untuk memastikan keamanan informasi perusahaan dapat terus dipertahankan.

Demikian journal singkat yang kami sampaikan, semoga bermanfaat. Terima kasih pada rekan dosen UIB yang telah memberikan motivai, serta PT. XYZ sebagai bahan evaluasi dan juga seluruh orang yang terlibat dalam penulisan journal ini.

References

Christopher. (2018). *Cyber Security.* New York: Saint.

Laudon, K., & P, J. (2007). *Sistem Informasi Manajemen.* Jakarta: Salemba Empat.

Nazir. (2008). *Metode Penelitian.* Bogor: Ghalia Indonesia.

Permatasari, M. (2000). Evaluasi Keamanan Sistem Informasi. *undib.ac.id*, 5.

Sarno, R., & Iffano. (2009). *Sistem Manajemen Keamanan Informasi.* Surabaya: ITSPress.