KAMPUS AKADMIK PUBLISING
Jurnal Ilmiah Research Student
Vol.1, No.3 Januari 2024
e-ISSN: 3025-5694; p-ISSN: 3025-5708, Hal 200-206
DOI: https://doi.org/10.61722/jirs.v1i3.564

EVALUASI KEAMANAN SISTEM INFORMASI MANAJEMEN PERUSAHAAN ASURANSI

Nonita Fitriani Harahap
Universitas Islam Negeri Sumatera Utara
Muhammad Irwan Padli Nasution
Universitas Islam Negeri Sumatera Utara

Alamat: Jln. Williem Iskandar Ps. V, Medan Estate, Kec.Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20371
Korespondensi penulis: nonitaharahap9@gmail.com

Abstract. Management information systems are transaction management can provide important information quickly, making it easier for management to retrieve it decisions in the interests of the company. An important aspect that is often forgotten in using the system information is a matter of information security. Information security is the protection of information which aims to protect from all sources of threats. The main principles of information security are confidentiality, data integrity and availability. Efforts to maintain In order to keep information safe, an evaluation of information security risks is needed which aims to identify threats and create mitigation plans to reduce risks. The agency's protection strategy is not working well because employees are not yet there receive training on information security. To improve security, companies must pay special attention attention to work on security policy, security organization, personnel security, physical and environmental security, communications and operations management, access control and compliance.
Keywords: *Information System Security; Company Management Information System.*

Abstrak. Sistem informasi manajemen merupakan manajemen transaksi yang dapat memberikan informasi penting dengan cepat, sehingga memudahkan manajemen untuk mengambil keputusan demi kepentingan perusahaan. Aspek penting yang sering dilupakan dalam penggunaan sistem informasi adalah masalah keamanan informasi. Keamanan informasi adalah perlindungan informasi yang bertujuan untuk melindungi dari segala sumber ancaman. Prinsip utama keamanan informasi adalah kerahasiaan, integritas data, dan ketersediaan. Upaya pemeliharaan Untuk menjaga keamanan informasi, diperlukan evaluasi terhadap risiko keamanan informasi yang bertujuan untuk mengidentifikasi ancaman dan membuat rencana mitigasi untuk mengurangi risiko. Strategi perlindungan badan tersebut tidak berjalan dengan baik karena karyawannya belum menerima pelatihan tentang keamanan informasi. Untuk meningkatkan keamanan, perusahaan harus memberikan perhatian khusus pada kebijakan keamanan, organisasi keamanan, keamanan personel, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, kontrol akses dan kepatuhan.
Kata Kunci: *Keamanan Sistem Informasi; Sistem Informasi Manajemen Perusahaan*

PENDAHULUAN

Teknologi Informasi merupakan elemen penting dalam kegiatan operasional perusahaan, tidak terkecuali perusahaan asuransi. Peran teknologi informasi pada aktivitas manusia pada saat ini memang begitu besar. Teknologi informasi telah menjadi fasilitas utama bagi kegiatan berbagai sektor kehidupan dimana memberikan andil besar terhadap perubahan-perubahan yang mendasar pada struktur operasional dan manajemen organisasi, serta penelitian. Dengan teknologi informasi, bisa menyederhanakan

Received November 30, 2023; Revised Desember 28, 2023; Januari 2, 2024
*

pekerjaan, memberikan nilai tambah dan mengurangi biaya transaksi dan proses penerbitan polis.

Keamanan Teknologi Informasi adalah aktivitas perlindungan sistem komputer dari serangan orang yang tidak bertanggungjawab. Termasuk di dalamnya pencegahan dari kerusakan pada hardware, software atau data elektronik, juga dari disrupsi atau misdirection dari layanan teknologi informasi. Keamanan teknologi informasi sering dikenal pula dengan istilah cybersecurity, information technology security (IT Security).

Peran keamanan sangat penting pada penggunaan teknologi informasi karena internet memungkinkan seorang hacker/cracker menyerang dari mana saja berada. Resiko yang terjadi akibat rendahnya tingkat keamanan adalah terjadinya pencurian data, kerugian finansial, pencurian identitas, kehilangan kepercayaan dari client, dan lain-lain. Teknologi dan sarana untuk melindungi sumber-sumber informasi antara lain Manajemen Identitas dan Autentisitas; Firewall, Sistem Deteksi Gangguan, dan Perangkat Lunak Antivirus; Melindungi Jaringan Nirkabel, Enkripsi dan Kunci Infrastruktur Publik; Menjaga Ketersediaan Sistem; Isu Keamanan Terhadap Cloud Computing dan Mobile Digital Platform; Menjaga Kualitas Perangkat Lunak.

METODE PENELITIAN

Metode yang dipakai dalam kajian ini adalah metode kualitatif karena menggunakan pendekatan deskriptif untuk mengidentifikasi ancaman potensial, kerentanan, dan dampaknya. Meskipun ini bersifat subjektif, dapat membantu dalam mengidentifikasi risiko tinggi dan prioritas perbaikan.

Metode ini mungkin lebih subjektif dibandingkan dengan metode kuantitatif, namun mereka masih dapat memberikan wawasan berharga tentang keamanan sistem informasi perusahaan asuransi. Hasil dari evaluasi kualitatif ini sering digunakan untuk merumuskan rekomendasi dan perbaikan keamanan yang lebih spesifik.

HASIL PENELITIAN DAN PEMBAHASAN

1. Pengertian Keamanan Informasi

Menurut Sarno dan Iffano keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi (return on investment. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sarno dan iffano : 2009).

Menurut ISO/IEC 17799:2005 tentang information security management system bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis.

Keamanan Informasi memiliki 3 aspek, diantaranya adalah :

1. Confidentiality, Confidentiality merupakan tindakan pencegahan dari orang atau pihak yang tidak berhak untuk mengakses informasi.
2. Integrity, Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari integrity adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak.

3. Availability, Keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Availability meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi.

2. Manajemen Keamanan Informasi

Aktifitas untuk menjaga agar perusahaan dan sumber daya informasi tetap aman disebut Manajemen keamanan informasi.

Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama, yaitu:

1. Kerahasiaan, melindungi data dan informasi perusahaan dari penyingkapan orang – orang yang tidak berhak
2. Ketersediaan, meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya.
3. Integritas, sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

Manajemen keamanan informasi (ISM) menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan. ISM terdiri dari empat langkah:

1. Identifikasi threats (ancaman) yang dapat menyerang sumber daya informasi perusahaan
2. Mendefinisikan resiko dari ancaman yang dapat memaksakan
3. Penetapan kebijakan keamanan informasi
4. Menerapkan controls yang tertuju pada resiko

Ancaman

a. Ancaman keamanan informasi adalah seseorang, organisasi, mekanisme, atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan
b. Ancaman dapat berupa internal atau external, disengaja atau tidak disengaja

Resiko

a. Pencurian dan Penyingkapan tidak sah
b. Penggunaan Tidak Sah
c. Pembinasaan dan Pengingkaran Layanan yang tidak sah
d. Modifikasi yang tidak sah

Teknologi dan Sarana untuk Melindungi Sumber-Sumber Informasi

1. Manajemen Identitas dan Autensitas

Autentisitas biasanya dibuktikan dengan menggunakan kata sandi yang hanya diketahui oleh pengguna yang berwenang. Teknologi autentisitas terbaru, seperti token, kartu pintar, dan autentisitas biometrik,mengatasi beberapa masalah terkini. Autentisitas biometrik menggunakan sistem yang dapat membaca dan menerjemahkan sifat perorangan manusia, seperti sidik jari, selaput pelangi mata, dan suara, untuk mengizinkan atau menolak akses.

2. Firewall, Sistem Deteksi Gangguan dan Perangkat Lunak Antivirus

a. Firewall

Firewall mencegah pengguna tidak berwenang dari mengakses jaringan privat.Pada organisasi besar, firewall biasanya diletakkan pada komputer yang

dirancang khusus dan terpisah dari sisa jaringan, sehingga tidak ada permintaan masuk secara langsung untuk mengakses sumber jaringan privat.

b. Sistem Deteksi Gangguan

Sistem deteksi gangguan mengutamakan alat pemonitor penuh waktu yang ditempatkan pada titik-titik paling rentan atau hot spot dalam jaringan perusahaan untuk mendeteksi dan menghalangi penyusup secara terus menerus.

c. Perangkat Lunak Antivirus dan Antispyware

Perangkat lunak antivirus harus dapat mencegah, mendeteksi, dan memindahkan malware, termasuk virus komputer, worms, trojan horses, spyware, dan adware. Untuk tetap efektif, perangkat lunak antivirus harus terus menerus diperbarui.

3. Melindungi Jaaringan Nirkabel

WEP atau *Wired Equivalent Privacy* yang menjadi standar keamanan wireless pertama kali sekarang dapat dengan mudah dipecahkan melalui berbagai sarana yang tersedia gratis di internet. Perbaikan atas kelemahan WEP ini memunculkan WPA2 atau Wi-Fi *Protected Access* 2 dengan standar keamanan yang lebih kuat, menggunakan lebih banyak kunci yang secara terus menerus berubah, membuatnya semakin sulit ditembus.

4. Enkripsi dan Kunci Infrastruktur Publik

Enkripsi merupakan proses transformasi teks dan data biasa menjadi teks tersandi yang tidak dapat dibaca oleh siapa pun kecuali pengirim dan penerima yang dituju. Dua metode untuk melakukan enkripsi lalu lintas jaringan pada web adalah SSL (*Secure Sockets Layer*) untuk membangun koneksi yang aman antara dua komputer dan S-HTTP (*Secure Hypertext Transfer Protocol*) untuk enkripsi data melalui internet, tetapi terbatas pada pesan individu.

5. Menjaga Ketersediaan Sistem

a. Pengendalian Lalu Lintas Jaringan : Inspeksi Paket Mendalam

Inspeksi paket mendalam menguji arsip data dan memilah materi online yang memiliki prioritas rendah dan menempatkan prioritas yang lebih tinggi untuk arsip bisnis yang penting.

b. Penggunaan Alih Daya untuk Keamanan

Managed Security Service Providers (MSSPs) memonitor aktivitas dan jaringan serta melakukan pengujian kerentanan dan deteksi gangguan melalui alih daya berbagai fungsi pengamanan.

6. Isu Keamanan Terhadap Cloud Computing dan Mobile Digital Platform

a. Keamanan dalam Cloud Computing

Pengendalian dapat dilakukan dengan menuliskan klausul keamanan *cloud computing* pada sebelum disetujui kontrak *Service Level Agreement* (SLA) dengan penyedia *cloud computing.*

b. Mengamankan Platform Mobile

Penggunaan perangkat mobile untuk banyak fungsi komputer harus diperlakukan sama-sama amannya seperti penggunaan PC desktop ataupun laptop. Perangkat mobile yang mengakses sistem dan data komputer membutuhkan perlindungan khusus dan perusahaan perlu memastikan bahwa kebijakan keamanan perusahaan termasuk perangkat ini dengan detail tambahan bagaimana perangkat mobile didukung, dilindungi, dan digunakan.

7. Menjaga Kualitas Perangkat Lunak

Matriks perangkat lunak merupakan penilaian objektif dari sistem dalam bentuk pengukuran yang terkuantifikasi. Pengujian perangkat lunak perlu dilakukan lebih awal, dilakukan secara reguler, dan ketat agar berkontribusi scara signifikan pada kualitas sistem. Pengujian yang baik dimulai bahkan sebelum program perangkat lunak ditulis dengan menggunakan walkthrough.

3. Langkah-Langkah Agar Keamanan Data Perusahaan Tetap Aman dan Terjamin

Berbeda dari ancaman fisik, ancaman *cyber* kerap terjadi di suatu perusahaan yang tidak terlalu peduli dengan keamanan jaringan dalam melakukan kegiatan ataupun mengakses sebuah informasi di dunia maya. Hal ini justru dapat menghambat perkembangan suatu perusahaan karena pegawai tidak dapat bekerja dengan optimal.

Dalam kondisi terburuk, serangan siber *(cyber)* juga dapat melumpuhkan suatu perusahaan jika terjadi pencurian sebuah data yang berhubungan dengan informasi finansial sehingga menimbulkan kerugian bagi perusahaan.

Sayangnya, tidak sedikit masyarakat Indonesia yang masih beranggapan bahwa keamanan data identik dengan perusahaan yang bergerak di bidang teknologi. Padahal, semua perusahaan yang memanfaatkan teknologi secara *online* dalam mengolah sebuah informasi, wajib memprioritaskan atau memberikan perhatian khusus dalam bidang keamanan siber ini.

Kini ada pentingnya, asosiasi negara-negara Uni Eropa sangat tanggap dalam menangani isu keamanan data dengan mengeluarkan berbagai regulasi, mereka meyakini bahwa kebocoran maupun pencurian data akibat kejahatan siber dapat memberikan dampak negatif bagi perusahaan serta dapat berimbas terhadap masalah perekonomian secara sistemik yang berdampak luas.

Oleh karena itu kamu harus melakukan strategi yang tepat dalam membuat kebijakan keamanan data perushaan sedini mungkin, Sobat Office! Lalu bagaimana cara untuk mengindari hal-hal yang tidak diinginkan tersebut? Ada beberapa langkah yang bisa kamu lakukan, di antaranya:

1. Membangun Infrastruktur IT yang Kokoh

Langkah awal yang dapat dilakukan adalah mengamankan infrastruktur di perusahaan tempat kamu berkerja, Sobat Office. Dengan infrastruktur yang kokoh artinya seluruh perangkat teknologi yang perusahaan miliki dapat dipastikan memilki perlindungan prima terhadap berbagai serangan siber. Dalam hal ini Tim IT perusahaan harus terus meng-*update* infrastruktur yang ada secara berkala agar terhindar dari berbagai ancaman keamanan lainnya.

2. Pastikan *Gadget* Selalu Aman

Tidak bisa dipungkiri keberadaan *gadget* atau *smartphone* saat ini sangat membantu dalam memfasilitasi akses data yang begitu cepat kapanpun dan di manapun. Salah satu hal yang dapat dilakukan adalah menggunakan aplikasi yang telah men-*support* data enkripsi seperti *Whatsapp* ataupun *Telegram* dalam membagikan sebuah informasi, dan kamu juga dapat menerapkan *password smartphone* yang kuat sehingga tidak mudah ditebak oleh orang lain.

3. *Backup Data Perusahaan Secara Berkala*

Dalam hal ini Sobat Office pastinya tidak bisa memprediksi kapan kegagalan sistem dapat terjadi ke depannya. Apa akibatnya jika hal tersebut terjadi? Tentu hal ini dapat merugikan perusahaan bukan? Memang secara tidak langsung tidak terlalu berkaitan dengan kejahatan siber, tetapi dengan menerapkan langkah ini tentu dapat

membantu memulihkan sebuah data yang dibutuhkan sewaktu-waktu jika terjadi ancaman siber. Pastikan tim IT tetap melakukan langkah ini secara rutin agar informasi yang di-*backup* selalu *up to date*.

4. **Gunakan Software Antivirus untuk Mendeteksi Ancaman**

   Langkah selanjutnya yang tidak kalah penting adalah memanfaatkan aplikasi/ *software* antivirus terpecaya yang dapat ditemukan di masing-masing *website* pelayanan antivirus yang legal. Dalam hal ini aplikasi Antivirus dapat mmberikan peringatan dini terhadap berbagai ancaman siber yang ada, sehingga berbagai kejanggalan aktivitas dapat terdeteksi dengan baik dan ancaman keamanan siber dapat dihindari.

5. **Evaluasi dan Audit IT Secara Berkala**

   Langkah terakhir yang wajib kamu lakukan adalah mengevaluasi langkah keamanan siber yang dilakukan perusahaan tempat kamu bekerja, Sobat Office. *How*? Yup, salah satunya adalah dengan melakukan Audit IT secara berkala. Langkah ini mampu memastikan sejauh apa kelemahan ataupun celah dalam sistem yang dimiliki perusahaan. Terdapat berbagai proses pengujian yang dapat kamu lakukan, misal seperti pengujian celah keamanan, pengetesan sistem dan sebagainya.

   Manfaatkan layanan Audit IT dari PT Integra Teknologi Solusi yang sudah terbukti dan tervalidasi oleh banyak sektor pemerintahan maupun BUMN. Didukung dengan tenaga ahli bersertifikasi internasional, PT Integra mampu memberikan pelayanan Audit IT dengan pengalaman terbaik yang pernah ada.

   Pada akhirnya keamanan data di era seperti sekarang ini sangatlah penting, karena semakin canggih perkembangan teknologi, semakin canggih pula kejahatan siber yang dapat mengancam keberlangsungan perusahaan.

KESIMPULAN

Teknologi informasi telah menjadi fasilitas utama bagi kegiatan berbagai sektor kehidupan dimana memberikan andil besar terhadap perubahan-perubahan yang mendasar pada struktur operasional dan manajemen organisasi, serta penelitian. Dengan teknologi informasi, bisa menyederhanakan pekerjaan, memberikan nilai tambah dan mengurangi biaya transaksi dan proses penerbitan polis.

Keamanan Teknologi Informasi adalah aktivitas perlindungan sistem komputer dari serangan orang yang tidak bertanggungjawab. Peran keamanan sangat penting pada penggunaan teknologi informasi karena internet memungkinkan seorang hacker/cracker menyerang dari mana saja berada. Resiko yang terjadi akibat rendahnya tingkat keamanan adalah terjadinya pencurian data, kerugian finansial, pencurian identitas, kehilangan kepercayaan dari client, dan lain-lain.

Manajemen keamanan informasi (ISM) menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan.

DAFTAR PUSTAKA

Putra, Y. M., (2018). Keamanan Informasi. *Modul Kuliah Sistem Informasi Manajemen.* FEB-Universitas Mercu Buana: Jakarta

Damayanti, K., Fardinal., (2019). The Effect of Information Technology Utilization, Management Support, Internal Control, and User Competence on Accounting Information System Quality. *Schollars Bulletin*, *5*(12), 751-758.

Hanifah, S., Sarpingah, S., & Putra, Y. M., (2020). *The Effect of Level of Education, Accounting Knowledge, and Utilization Of Information Technology Toward Quality The Quality of MSME ' s Financial Reports*. *The 1st Annual Conference Economics, Business, and Social Sciences (ACEBISS) 2019*,

T. Thoyyibah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X," J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf., vol. 4, no. 2, p. 72, 2018, doi: 10.24014/coreit.v4i2.6292.

T. Kristanto, M. Sholik, D. Rahmawati, and M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ," JISA(Jurnal Inform. dan Sains), vol. 2, no. 2, pp. 30–33, 2019, doi: 10.31326/jisa.v2i2.497.

https://integrasolusi.com/blog/tips-ini-langkah-langkah-agar-keamanan-data-perusahaan-tetap-aman-terjamin/

https://www.cbqaglobal.com/strategi-dan-evaluasi-cyber-security-iso-27001/

https://itgid.org/manajemen-keamanan-informasi-perusahaan/