INCODING: Journal of Informatic and Computer Science Engineering

https://journal.mahesacenter.org/index.php/incoding/index || ISSN 2776-432X (online)

2 (1) 2022: 21-30

DOI:10.34007/incoding.v2i1.244 **Submitted: 16-03-2022 , Reviewed: 16-03-2022, Accepted: 11-04-2022**

Penerapan Sistem Keamanan Informasi Pada Perusahaan PT. XYZ

Application of Information Security Systems at PT. XYZ

Andri Darmawan[1)]*

1)Prodi Teknologi Rekayasa Komputer, Politeknik LP3I Medan, Indonesia

*Coresponding Email: andridarmawan@plm.ac.id

Abstrak

Informasi merupakan salah satu aset bisnis perusahaan yang penting, dan sudah seharusnya dilindungi dengan baik. Keamanan informasi perusahaan turut menentukan kelangsungan bisnis, mengoptimalkan keuntungan perusahaan, juga melindungi dari resiko yang dapat membahayakan bisnis itu sendiri. Keamanan informasi dapat diterapkan dengan cara mengimplementasikan satu set kontrol berupa aturan, prosedur, struktur organisasi dan penggunaan software. Kontrol-kontrol ini perlu dibangun untuk memastikan bahwa tujuan keamanan informasi perusahaan dapat tercapai. Artikel ini memberikan rekomendasi seperangkat information security policy menurut ISO/IEC 17799:2000 pada perusahaan IT PT. XYZ yang bergerak dalam bidang Teknologi Informasi. Rekomendasi dibuat berdasarkan kajian ilmiah dan disesuaikan dengan kebutuhan perusahaan tersebut. Hasil dari Proyek Akhir ini dapat dijadikan acuan bagi perusahaan sejenis untuk menyempurnakan standar keamanan informasi pada lingkungan bisnisnya.

Kata Kunci: sistem keamanan, keamanan informasi, sistem informasi, IT, security.

Abstract

Information is an asset that, like other important assets, has value to an enterprise and consequently needs to be well protected. Information security practices protect information from a wide range of threats in order to guarantee business continuity, minimize business losses, and maximize profit and business opportunities. Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that specific security objectives of the organization are met. This Final Project produces a set of information security policies for the case of PT. XYZ, which complies with the standard ISO/IEC 17799:2000. These policies are established to meet the needs of PT. XYZ based on scientific studies. The result of this research can be used as a reference for enterprises with similar business domain as PT. XYZ.

Keywords*: security system, information security, information system, IT, security.*

PENDAHULUAN

Manajemen Resiko (Risk Management) merupakan proses yang cukup sulit dan menghabiskan waktu yang tidak sedikit. Dibutuhkan keahlian, keuletan, latihan, dan perbaikan secara berterusan. Tetapi hasil usaha yang dikerjakan pada tahap ini, akan memberikan input yang berharga bagi perusahaan, yakni menekan ketidakpastian, dan membantu kesiapan perusahaan dalam menghadapi tantangan bisnis masa depan. Risk Management merupakan sebuah proses yang tak kenal henti dan penuh tantangan. Ada perhitungan matematis, tapi justru imajinasi dan kreatifitas yang akan banyak berperan – pada kasus ini, adalah untuk melihat dan mengantisipasi perkembangan bisnis serta dampak bisnis dari keputusan yang diambil. Kelangsungan proses manajemen resiko adalah continously improving, terus dan berkelanjutan. Perusahaan berusaha memastikan bahwa hal-hal yang tidak diinginkan tidak terjadi, atau apa pun yang terjadi perusahaan tetap dapat bertahan dan mengembalikan proses dan fungsi bisnis pada posnya masing-masing.

PT XYZ merupakan perusahaan yang bergerak di bidang layanan IT. Customer PT. XYZ tersebar di beberapa daerah di Indonesia seperti Medan, Palembang, Bandung, Ambon dan tentu saja ibukota Jakarta. Layanan yang diberikan berupa pengembangan perangkat lunak, pengimplementasian jaringan dan atau infrastruktur sistem informasi, dan penyediaan Disaster Recovery Center. Diantaranya seperti pengembangan Sistem Informasi Dana Pensiun, Pajak Online, Sistem Informasi SDM, Sistem Informasi Asuransi, Server Co□Location dan banyak lagi. Jika mengacu kepada kebijakan yang diterapkan PT XYZ, ternyata masih sedikit aturan-aturan yang dibuat untuk mengatasi kendala pengamanan informasi perusahaan. Ada celah-celah yang memungkinkan terjadinya kesalahan, diantaranya disebabkan oleh 1. Pemberian wewenang yang tidak jelas, contohnya ada beberapa personal yang mengetahui password server produksi sedangkan personal tersebut tidak memiliki tanggung jawab pada server tersebut; server produksi dipergunakan untuk belajar sehingga rawan kesalahan yang dapat membahayakan sistem keseluruhan. 2. Terjadinya pencurian data atau aplikasi karena lokasi server yang terbuka, dan dapat diakses oleh siapa saja. 3. Tidak adanya prosedur yang jelas, tertulis, dibakukan dan disahkan oleh perusahaan untuk melakukan pekerjaan tertentu bagi operator sehingga terkadang operator menggunakan metode trial and error. Oleh sebab itu pembuatan kebijakan perusahaan yang berkaitan dengan

keamanan sistem informasi dan berdasarkan standar keamanan internasional sangat dibutuhkan.

Belum adanya kebijakan perusahaan yang baku dalam mengamankan sistem informasi yang berkaitan dengan informasi internal maupun eksternal perusahaan, sehingga dirasa perlu untuk melakukan audit, analisa dan merancang ulang kebijakan perusahaan yang telah ada atau belum ada dengan mengacu pada standar keamanan informasi ISO/IEC 17799:2000. Tujuan dari penelitian ini adalah untuk menjelaskan cara agar dapat menekan tingkat ketidakpastian kondisi masa depan, mengatur informasi, sebagai aset terpenting organisasi, bebas dari resiko. Memperbaiki keamanan sistem informasi yang dimiliki PT. XYZ sehingga mampu memberikan jaminan keamanan informasi baik informasi internal maupun eksternal perusahaan, menganalisa kelemahan-kelemahan keamanan informasi perusahaan dan memberikan rekomendasi pemecahan masalah-masalah yang bisa dilakukan untuk membuat keamanan sistem informasi lebih aman dan memberikan rekomendasi rancangan kebijakan perusahaan guna meningkatkan keamanan sistem informasi PT. XYZ. Semua tujuan dari penelitian ini mengacu pada standar information security ISO/IEC 17799:2000.

METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah a. Studi Literatur yang terkait dengan kemanan system informasi. Studi ini dilakukan dari berbagi sumber seperti, buku-buku, jurnal-jurnal termasuk dokumen-dokumen elektronik yang ada di Internet. Selain itu studi juga dilakukan pada dokumen-dokumen yang ada dalam perusahaan terutama dokumen-dokumen yang berkaitan dengan keamanan sistem informasi. b. Observasi dilakukan secara langsung dengan mendatangi lokasi Data Center PT. XYZ dan menganalisa kemungkinan adanya kelemahan kelemahan dari keamanan sistem tersebut. c. Wawancara informal yang dilakukan pada personal-personal yang terlibat dan bertanggung jawab dalam sistem informasi PT. XYZ.

HASIL DAN PEMBAHASAN

Pembuatan sistem keamanan informasi merupakan proses yang terus berkelanjutan, dan tidak pernah berhenti seiring perkembangan bisnis perusahaan,

organisasi dan perkembangan teknologi. Proses pengembangan sistem membutuhkan waktu, anggaran khusus dan dukungan dari semua elemen perusahaan untuk mendukungnya. Apa yang dituliskan di sini tidak menggambarkan keseluruhan fungsi-fungsi yang ada pada PT XYZ, melainkan mengambil kasus pada salah satu departemen, yakni Data Center Department. Tujuan Proyek Akhir ini adalah sebagai pembuka jalan dalam usaha membangun sistem keamanan informasi pada PT XYZ. Dampak yang diharapkan adalah terbangunnya budaya organisasi untuk turut mengembangkan dan menjaga sistem keamanan informasi perusahaan.

Penjelasan Kebijakan Keamanan Informasi

PT. XYZ dalam pelayanannya kepada klien dan rekan bisnis selalu melibatkan sistem yang dapat menjamin keamanan informasi. Perkembangan hardware dan software yang terus berubah seiring dengan semakin majunya teknologi informasi, telah berulang kali membuktikan perlunya kerja berkesinambungan untuk mendukung keamanan dan eksistensi perusahaan. PT. XYZ dalam menawarkan jasa dan produknya, ingin agar klien dan rekan bisnisnya merasa aman dan yakin bahwa investasi yang ditanamkan tidak sia-sia. Tugas utamanya adalah memastikan meningkatnya kualitas pelayanan, yang harus ditunjukkan oleh tiga hal: karyawan, rekan bisnis, dan contoh dari tubuh perusahaan sendiri. Karyawan adalah aset PT. XYZ yang paling berharga. Merekalah yang akan menentukan maju mundurnya perusahaan. Maka dari itu pihak perusahaan berusaha untuk menyediakan atmosfer kerja yang baik, dan memotivasi mereka untuk meningkatkan pengetahuan tentang keamanan informasi. Untuk mendapatkan kualitas yang terjaga dalam seluruh proyeknya, PT. XYZ hanya akan bekerjasama dengan rekan bisnis yang telah diseleksi, agar resiko kerja yang tidak profesional dapat diminimalkan, dan mendapatkan komitmen tinggi untuk memberikan realisasi yang terbaik. Terakhir yang juga penting adalah memberikan contoh keamanan informasi dan jaringan (information and network security) dalam tubuh PT. XYZ sendiri. PT. XYZ dapat memastikan bahwa informasi dan aset lainnya dalam status aman dan terlindung, menunjukkan bahwa PT. XYZ merupakan contoh yang baik selaku perusahaan yang keamanan informasinya tertata dengan baik. Setiap klien yang datang, dipastikan dapat melihat bahwa PT. XYZ memiliki Sistem Keamanan Informasi yang handal. PT. XYZ akan menyediakan dokumentasi yang mencukupi. Kebijakan

Penanganan Informasi (Information Handling Policy), akan menjelaskan perlindungan terhadap informasi strategis yang akan dilakukan oleh pengguna internal dan eksternal. Kebijakan Password (Password Policy) akan menjelaskan bagaimana membuat, menyimpan dan mengubah password. Kebijakan Transfer Informasi (Information Transfer Policy) akan menerangkan siapa yang bertanggung-jawab untuk melakukan instalasi dan modifikasi software pada mesin-mesin produksi milik perusahaan. Beberapa elemen Sistem Keamanan Informasi – contohnya: hak akses, password, user account - akan disertakan dalam prosedur kerja karyawan, dan setiap pelanggaran yang dilakukan akan dikenai sanksi. Kebijakan Transfer Informasi menjelaskan siapa yang bertanggung-jawab untuk melakukan instalasi dan modifikasi software pada mesin-mesin produksi.

Untuk memastikan sistem berjalan sesuai rencana, Dewan Direksi akan menugaskan secara khusus satu orang sebagai penanggung-jawab keseluruhan kegiatan sistem. Tujuannya adalah mengimplementasikan dan memelihara sistem keamanan informasi secara baik dan benar.

Menentukan Cakupan ISEC System

PT. XYZ adalah perusahaan yang begerak di bidang layanan IT. Awalnya dibangun untuk memenuhi kebutuhan IT pada sebuah bank di Indonesia. Sejak 1995 perusahaan ini mengembangkan usahanya untuk memasuki lapangan bisnis selain dunia perbankan. Adapun bidang usaha yang dimasuki adalah: pemrograman aplikasi, pengembangan intranet / internet, jasa layanan dokumen, sistem integrasi jaringan komunikasi data, pemeliharaan perangkat keras dan jaringan komunikasi data, jasa konsultasi IT, business intelligent, dan enterprise management. PT. XYZ terdiri dari beberapa departemen dengan spesifikasi keahlian sebagai berikut: programmer, system analyst, system engineer, quality assurance, network engineer, operator, customer support, helpdesk, user liaison, *security administration* dan *consultan.* Saat ini tercatat lima orang System Engineer dan tiga orang operator, selain Data Center Manager yang tergabung dalam Data Center Department (struktur organisasi dapat dilihat pada lampiran). Aset perusahaan yang diamanahi cukup besar yakni: router, firewall, beberapa Intel compatible server, IBM S/390, IBM 3746, IBM 2074, dan IBM 3494. Namun demikian

belum ada pengalaman, kecuali kebijakan-kebijakan umum yang diterapkan kepada seluruh tamu maupun karyawan perusahaan. Contohnya sebagai berikut:

1. Tidak diperkenankan membawa makanan / minuman ke dalam ruang Data Center.

2. Ruang Data Center harus selalu terkunci.

3. Setiap pengunjung wajib menuliskan keterangan keperluan kunjungan pada buku tamu, walaupun berstatus sebagai karyawan internal perusahaan.

4. Tiap orang yang memiliki hak akses ke Data Center harus didaftarkan oleh grup operasional / operator.

5. Ruang Data Center tidak boleh kosong atau tidak ada orang selama 24 jam non-stop, sehingga jika ada waktu istirahat dilakukan secara bergantian.

6. Temperatur Data Center harus dipertahankan pada level di bawah 22° C.

7. Setiap hari keadaan temperatur harus dibuat laporannya.

8. Melakukan analisa terhadap temperatur yang berubah atau melewati batas yang telah ditetapkan, untuk selanjutnya diambil tindakan agar hal tersebut tidak terjadi kembali.

9. Perangkat yang masuk Data Center harus mempunyai data-data yang lengkap yakni:

a. Software dalam perangkat tersebut.

b. Fungsi perangkat.

c. Spesifikasi perangkat.

d. Bagaimana mengoperasikannya, apakah cukup operator, atau langsung pihak yang menitipkan perangkat tersebut.

e. Berapa kebutuhan tenaga / power / listrik.

f. Berapa temperatur yang dibutuhkan.

Cakupan ISEC System yang baik tentunya meliputi semua kebutuhan keamanan informasi perusahaan, namun seperti yang telah dituliskan dalam batasan masalah maka cakupan ISEC System yang akan dibangun pada Proyek Akhir ini meliputi Information Security Policy dan Organizational Security. Namun demikian baik prosedur, kebijakan, dan instruksi yang dibuat terkait juga dengan:

1. Asset Classification and Control, yakni prosedur manajemen resiko.

2. Access Control, yakni prosedur pembuatan dan pemeliharaan user account, instruksi pembuatan file pribadi, prosedur pembatalan hak akses mantan karyawan, instruksi pembuatan daftar akses, dan instruksi pembuatan database pengguna.

3. Communications and Operations Management, yakni kebijakan transfer informasi.

4. Compliance, yakni prosedur dan rencana audit.

Analisa dan Manajemen Resiko

Tahap selanjutnya adalah melakukan analisa resiko, lebih lengkap dapat dilihat pada lampiran analisa resiko. Seperti telah dijelaskan pada bab-bab sebelumnya, metode analisa resiko yang digunakan pada kasus ini adalah metode kuantitatif yakni metode yang menggunakan angka untuk mendeskripsikan keadaan pada PT. XYZ. Tahap pertama dalam melakukan analisa resiko adalah melakukan identifikasi aset-aset informasi milik perusahaan. Aset-aset tersebut dapat dilihat pada tabel 1.

Tabel 1. Daftar Aset

No	Daftar Aset
Aset Informasi	
1	Dokumentasi SNA Server
2	Dokumentasi Linux SuSE S/390
3	Dokumentasi Linux SuSE S/390
4	Dokumentasi Print Procedure
5	Surveilance Operation Manual
6	Fire System Operation Manual
7	UPS Operation Manual
8	Disaster Recovery Plan
Aset Software	
1	Linux SuSE SLES 7 for S/390
2	OS/390 V.2.10
3	DB2 UDB V.8.1 for Linux S/390
4	Lotus Domino Mail Server
5	WebSphere Application Server V.5.0 for Linux S/390
6	Windows NT 4.0
7	Windows 2000 Professional
8	Windows XP
9	Linux SuSE Professional 7.2 for Intel
10	IBM HTTP Server
11	PuTTY Release 0.52
12	Squid V.2.5-Stable
13	Nexus Mainframe Terminal
14	Lotus Notes
Aset Fisik	
1	Nortel Contivity 1700 VPN Server
2	IBM Mainframe S/390 G6

3	IBM 3746 Communication Controller
4	IBM 2074 Terminal Server
5	IBM 3494 Tape
6	Intel Print Server
7	Intel ICS Server
8	Intel Development Server
9	Hard Drive
10	CD ROM
11	Network Card
12	Disks
13	Disk Drive
14	Switch / Hub
15	Router
16	Intel Camera Server
17	Intel Fax Server

Jika kita lihat, maka urutan poin-poin tertinggi yang diperlihatkan pada tabel analisa resiko (lihat lampiran analisa resiko) menunjukkan urutan sebagai berikut: 1. Disable mail relaying (20 poin). 2. Kebijakan password (16 poin). 3. Membatasi akses pengguna (16 poin). 4. Information Transfer Policy (12 Poin) . 5. Check disk space secara periodik, install antivirus (12 poin). 6. Membeli / menyiapkan cadangan perangkat, e-signature (12 poin). 7. Server diletakkan dalam rak terkunci (12 poin). 8. Enkripsi data, mengupdate software dengan versi terbaru (8 poin). 9. Gunakan system command untuk mematikan mesin (8 poin). 10. Backup periodik (8 poin). 11. Asuransi (8 poin). 12. Siapkan anggaran untuk mengganti perangkat (8 poin). 13. Menempatkan perangkat dengan baik dan benar (4 poin). Perusahaan dapat menerima, menghindari, mentransfer, atau pun menekan resiko yang dihadapi. Sebagai langkah lanjutan, yakni manajemen resiko, maka daftar di atas merupakan daftar urutan tindakan-tindakan pencegahan dan penyelamatan (safeguards) yang menjadi rekomendasi untuk dilakukan oleh perusahaan. Perusahaan sebaiknya segera melakukan tindakan-tindakan tersebut untuk menekan resiko yang mungkin terjadi.

Menentukan *Control Objectives* dan *Controls*

Walaupun ISO 17799 merekomendasikan untuk menerapkan semua daftar kontrol yang tercantum, namun hal ini bukanla sesuatu yang wajib diikuti. Kebebasan sepenuhnya diberikan kepada pihak manapun yang hendak mengadopsi kontrol-kontrol pada ISO 17799. Seperti yang telah dituliskan dalam batasan masalah maka cakupan ISEC System yang akan dibangun pada Proyek Akhir ini meliputi Information Security Policy dan Organizational Security.

Membuat Kebijakan-Kebijakan

Tahap terakhir dari proses pembangunan ISEC System adalah membuat kebijakan-kebijakan. Selanjutnya kebijakan, prosedur dan instruksi dapat dilihat pada lampiran. Adapun poin-poin yang akan dibuat meliputi 6 poin prosedur, 3 poin kebijakan, dan 5 buah instruksi sebagai berikut:

1. Prosedur Pembuatan Kebijakan Keamanan Informasi
2. Prosedur Pembuatan Dan Pemeliharaan User Account
3. Prosedur Pembatalan Hak Akses Mantan Karyawan
4. Prosedur Pemeliharaan Sistem Komputer
5. Prosedur Manajemen Resiko
6. Prosedur Audit
7. Rencana Audit
8. Kebijakan Password
9. Kebijakan Transfer Informasi
10. Kebijakan Penanganan Informasi
11. Instruksi Pembuatan File Pribadi
12. Instruksi Pembuatan Daftar Akses
13. Instruksi Pembuatan Database Pengguna
14. Instruksi Ketika Keadaan Darurat
15. Instruksi Penanganan Insiden Keamanan

SIMPULAN

Berdasarkan pengamatan terhadap Data Center Department di PT. XYZ dapat disimpulkan bahwa penelitian ini telah membuat seperangkat kebijakan, prosedur, instruksi dan rekomendasi sistem keamanan informasi PT. XYZ. Penerapan perangkat ini dapat memperbaiki keamanan sistem informasi milik PT. XYZ sekaligus membantu menyelesaikan masalah-masalah yang dihadapi PT. XYZ berkaitan dengan sistem keamanan informasi. Untuk mengoptimalkan keamanan sistem informasi di perusahaan, diperlukan implementasi peraturan berupa security policy yang harus disosialisasikan, dipatuhi dan didukung oleh seluruh elemen perusahaan. Security policy harus dipahami sebagai suatu aset penting, yang selain melindungi sistem informasi milik perusahaan juga melindungi karyawan semua. Hasil dari penelitian ini dapat dijadikan acuan bagi

perusahaan sejenis untuk menyempurnakan standar keamanan informasi pada lingkungan bisnisnya.

DAFTAR PUSTAKA

[1] Caelli W., Longley D., Shain M. Information Security Handbook Macmillan Publishers Ltd., 1991.
[2] CNN, Insufficient computer security threatens doing business online http://www.cnn.com, 23 Februari 2000.
[3] CNN, Highly classified' State Department computer missing http://www.cnn.com, 17 April 2000.
[4] CNN, State Department missing 15 unclassified laptop computers http://www.cnn.com, 18 Mei 2000.
[5] Kurniawan, Eko. Audit, Analisa dan Perancangan Infrastruktur Network Security - Studi Kasus: Mobile Internet Service Company, 2003.
[6] Finne, T. Analyzing Information Security: Knowledge-Based DSS Approach Åbo Akademi University Institute for Advanced Management Systems Research Finland, 1996.
[7] Rent-a-hacker http://www.rent-a-hacker.com, 2001.
[8] Riyadi, Hendra. Pengembangan Kebijakan Kemananan Teknologi Informasi Jaringan Komputer pada PT. X, 2003.
[9] ISO IEC TR 13335-3/1998. Information technology - Guidelines for the management of IT Security: Part 3: Techniques for the management of IT Security http://www.iso.ch , 1998.
[10] International Standard ISO/IEC 17799, 2000.
[11] ITSEC. Information Technology Security Evaluation Criteria Commission of European Communities, 1991.
[12] Krutz, Ronald L., Vines, Russel Dean. The CISSP Prep Guide Wiley, 2001.
[13] Raftery, J. Risk Analysis in Project Management, 1994.
[14] Smith, M. R. Commonsense Computer Security, McGraw-Hill, 1993. 56
[15] Stallings, W. Cryptography and Network Security, Third Edition Prentice Hall, 2002.
[16] Syta, Jakub A. The Project of Information Security System based on ISO 17799 regulations for AVET INS Warsaw, 2001.
[17] GAO, Executive Guide: Information Security Management United State General Accounting Office, 1998.
[18] Vigilinx. White Paper: Security Assessment Methodology http://www.vigilinx.com, 2001.