Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Menggunakan METODE FMEA Dan ISO 27001

Tata Satria Timor Perdana

Jurusan Sistem Komputer, Universitas Sriwijaya
Jl. Srijaya Negara Asrama Brimob Bukit Besar, Kota Palembang, Sumatera Salatan, Indonesia

Email : tatasatriatp@gmail.com

ABSTRAK

Penggunaan Teknologi Informasi di lembaga-lembaga pemerintahan saat ini sangat dibutuhkan untuk mempermudah melakukan pendataan dan pengambilan keputusan yang strategis. Kantor Pelayanan Pajak yang merupakan salah satu lembaga pemerintahan yang bergerak dibidang keuangan memiliki data yang cukup banyak. Penggunaan Teknologi informasi bukan sekedar penting tapi sudah menjadi keharusan, melihat Pajak merupakan salah satu pendapatan negara yang utama. Data dan informasi yang terdapat pada Lembaga ini tidak hanya perlu penyimpanan secara digital akan tetapi juga memerlukan pengamanan yang serius. Kebocoran akan data yang ada dapat berakibat fatal bagi kepentingan negara. Untuk itu Sistem Manajemen Keamanan Informasi(SMKI) diperlukan dalam pengelolaan keamanannya. Dalam mengimplementasikan ISO 27001 sebelumnya diperlukan manajemen resiko keamanan informasi. Kegiatan manajemen resiko ini diperlukan untuk menentukan Control Objectives yang akan diambil untuk melakukan penanganan resiko yang kemungkinan terjadi. Dalam mengimplementasikan manajemen resiko didapatkan hasil hanya pada aset username dan password level yang resikonya High (6,67%) dari 15 aset yang sudah terdaftar, sehingga diperlukan kontrol keamanan yang berhubungan dengan username dan password untuk meminimalisir atau mengurangi terjadinya resiko.
Kata Kunci: Manajemen resiko,SMKI, iso 27001

ABSTRAK

ANALYSIS OF INFORMATION SECURITY RISK MANAGEMENT IN TAX SERVICE OFFICE

Use of Information Technology in government institutions at this time is needed to make it easier to collect data and strategic decision making. KPP which is one of the government agencies engaged in finance have enough data. The use of information technology is not just important but has become imperative, see Tax is one of the main income of the country. The data and information contained in this Organization not only need a digital storage but also require security seriously. Leakage will be the existing data can be fatal to the interests of the state. For the Information Security Management System (ISMS) is required in the management of safety. In previously required to implement ISO27001 information security risk management. Risk management activities is necessary to determine the Control Objectives that will be taken to have addressed the risk probabilities. In implementing risk management on assets showed only a username and password High risk level (6,67%) of 15 assets that are registered, so that the necessary security controls associated with a username and password to minimize or reduce the risk.
Keywords: Risk Management,SMKI, ISO 27001.

1. PENDAHULUAN

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan exportimport,tranportasi, lembaga keuangan, pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting). Informasi atau data adalah asset bagi perusahaan. Keamanan data secara tidak langsung dapat

memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekseposnya data ke pihak eksternal yang tidak diinginkan. Bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspose, melatarbelakangi disusunnya ISO17799, standar untuk system manajemen keamanan informasi. [1]

Keamanan informasi terdiri dari perlindungan terhadap aspek aspek berikut:

1. Confidentiality (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. Integrity (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. Availability (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).[2]

2. Metode

Pada pembahasan ini akan dijelaskan metodologi dalam penelitian ini mulai dari pengumpulan data untuk melakukan identifikasi aset, melakukan perhitungan Nilai aset yang telah dikumpuklan,melakukan identifikasi ancaman dan kelemahan aset, melakukan analisa dampak bisnis atau yang sering disebut Business Impact Analysis (BIA), melakukan identifikasi level resiko dan yang terakhir menghitung risk value untuk mengetahui level resiko dari aset. Tahap awal penelitian ini adalah mengumpulkan data asset yaitu aset yang mengandung data dan atau informasi. Identifikasi Aset dilakukan untuk menentukan asset yang berhubungan dengan control akses di KPP Pratama XYZ. Setelah aset teridentifikasi, langkah selanjutnya yaitu melakukan perhitungan nilai aset. Pendekatan yang dilakukan dengan menggunakan tiga aspek keamanan, yaitu kerahasiaan (confidentiality),keutuhan (Integrity) dan ketersediaan (availiability). Setelah mendapatkan nilai resiko, level resiko didapatkan dengan menyesuaikan nilai resiko dengan Tabel 5 Matrik Level Resiko. Hasil yang didapatkan setiap aset akan teridentifikasi tingkat level resikonya. Level resiko berdasarkan Tabel tersebut menunjukkan Low,Medium atau High. Dari hasil tersebut aset yang akan dilakukan pengelolaan resiko adalah aset yang beresiko High.[3]

3. Landasan Teori

1. KEAMANAN INFORMASI

Saat pemerintah dan kalangan industri mulai menyadari kebutuhan untuk mengamankan sumber daya informasi mereka, perhatian nyaris terfokus secara eksklusif pada perlindunga peranti keras data maka istilah keamanan sistem digunakan. Istilah keamanan sistem digunakan untuk mengambarkan perlindungna baik peralatan komputer dan nonkomputer, fasilitas,data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang.

Tujuan Keamanan Informasi

- Keamanan informasi ditujuakan untuk mencapai tiga tujuan utama yakni:

Kerahasiaan. Perusahaan berusaha untuk melindungi data dan informasinya dari pengungkapan orang-orang yang tidak berwenang.

- Ketersediaan. Tujuan dari infrastruktur informasi perusahaan adalah menyediakan data dan informasi bagi pihak-pihak yang memiliki wewenang untuk menggunakannya.Integritas. Semua sistem informasi harus memberikan representasi akurat atas sistem fisik yang direpresentasikannya.

2. Manajemen Keamanan informasi

Aktivitas untuk menjaga agar sumber daya informasi tetap aman disebut manajemen keamanan informasi (information security management – ISM), sedangkan aktivitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah adanya bencana disebut manajemen keberlangsungan bisnis (bussiness continuity management – BCM).

Jabatan direktur keamanan sistem informasi perusahaan (coorporate information system security officer – CISSO) digunakan untuk individu di dalam organisasi, biasanya anggota dari unit sistem informasi yang bertanggung jawab atas keamanan sistem informasi perusahaan tersebut.

3. MANAJEMEN KEAMANAN INFORMASI

Pada bentuknya yang paling dasar, manajemen keamanan informasi terdiri atas empat tahap yakni:

a. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
b. Mendefenisikan risiko yang dapat disebabkan oleh ancaman-ancaman tersebut
c. Menentukan kebijakan keamanan informasi
d. Mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut.

Istilah manajemen risiko (risk management) dibuat untuk menggambarkan pendekatan ini dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.

Tolak ukur (benchmark) adalah tingkat kinerja yag disarankan. Tolak ukur keamanan informasi (information security benchmark) adalah tingkat kemanan yang disarankan yang dalam keadaan normal harus menawarkan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi.standar atau tolak ukur semacam ini ditentukan oleh pemerintah dan asosiasi industri serta mencerminkan komponen-komponen program keamanan informais yang baik menurut otoritas tersebut.[1]

Ketika perusahaan mengikuti pendekatan ini, yang disebut kepatuhan terhadap tolak ukur (benchmark compliance) dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolak ukur tersebut menawarkan perlindungan yang baik.

4. RISIKO

Risiko Keamanan Informasi (Information Security Risk) didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Risiko-risiko seperti ini dibagi menjadi empat jenis yaitu:

- Pengungkapan Informsi yang tidak terotoritasis dan pencurian. Ketika suatu basis data dan perpustakaan peranti lunak tersedia bagi orang-orang yang seharusnya tidak memiliki akses, hasilnya adalah hilangnya informasi atau uang.
- Penggunaan yang tidak terotorisasi. Penggunaan yang tidak terotorisasi terjadi ketika orang-orang yang biasanya tidak berhak menggunakan sumber daya perusahaan mampu melakukan hal tersebut.

4. Hasil dan pembahasan

Berdasarkan pengambilan data dengan wawancara dan observasi di KPP XYZ
didapatkan data aset seperti terlihat pada Gambar 1. Daftar Aset dibagi menjadi jenis Aset yang terdiri dari perangkat keras, perangkat lunak dan Data.

No	Jenis Aset	Aset
1	Perangkat Keras	PC, Server, Jaringan fisik Kabel , Kamera CCTV,DVR CCTV Cisco Router
2	Perangkat Lunak	ESPT,EFAKTUT,EFILING,EBILING, SIM-Kepegawaian, SIM-WP, SIM-Pajak,WEB-Server
3	Data	Username dan Password

Gambar.1

Dari data aset yang telah didapatkan selanjutnya menghitung nilai aset, dan dari hasil observasi dan wawancara didapatkan nilai asset yang teridentifikasi seperti gambar 2 dibawah ini.

Langkah selanjutnya adalah mengidentifikasi kelemahan dan ancaman untuk mendapatkan Nilai Threat (NT). Hasil identifikasinya terlihat pada Gambar 3.

No	Aset	Kriteria			Nilai Aset
		NC	NI	NV	
1	PC	2	1	2	5
2	Server	4	4	4	12
3	Jaringan Fisik Kabel	3	2	3	8
4	Kamera CCTV	2	2	2	6
5	DVDR CCTV	2	2	2	6
6	Cisco Router	3	2	4	9
7	ESPT	3	3	3	9
8	EFAKTUT	3	3	3	9
9	EFILLING	3	2	3	8
10	EBILLING	3	2	2	7
11	SIM-Kepegawaian	2	2	2	6
12	SIM-WP	2	2	3	7
13	SIM-Pajak	3	3	3	9
14	Web Server	4	3	3	10
15	Data User dan Password	4	3	3	10

Gambar.2

Aset	Kejadian	Jenis ancaman/ kelemahan	Prob. (low/ med/ high)	Event	Nilai Prob.	∑ PO	NT
PC	Pencurian PC	ancaman	low	0	0	0	-
Server	Pencurian PC	ancaman	low	0	0	0	-
	Illegal Akses	ancaman	low	0	0		
Jaringan	Illegal Akses	ancaman	low	0	0	0	-
	Pencurian PC	ancaman	low	0	0		
Kamera CCTV	Pencurian PC	ancaman	low	0	0	0	-
	Perusakan	ancaman	low	0	0		
DVDR CCTV	Pencurian Perangkat	ancaman	low	0	0	0	-
	Perusakan	ancaman	low	0	0		
	Pencurian Rekaman	ancaman	low	0	0		
Cisco Router	Illegal Akses	ancaman	low	0	0	0	-
	Pencurian	ancaman	low	0	0		
ESPT	Aplikasi tidak terupdate	kelemahan	low	0	0	0.4	0.13
	serangan Virus	ancaman	low	3	0.15		
	Kegagalan Operasional	kelemahan	low	5	0.25		

Gambar.3

Setelah melakukan dentifikasi ancaman dan kelemahan sehingga mendapatkan hasil Nilai ancaman (NT), langkah selanjutnya adalah dengan menentukan nilai BIA dari masing-masing aset. Dari hasil observasi didapatkan nilai BIA

seperti terlihat pada Gambar 4.Langkah selanjutnya yaitu menghitung Nilai Resiko dari NA, BIA dan NT yang sudah didapatkan.

Aset	Nilai BIA
PC	1
Server	4
Jaringan Fisik Kabel	2
Kamera CCTV	1
DVDR CCTV	1
Cisco Router	3
ESPT	2
EFAKTUT	2
EFILLING	2
EBILLING	2
SIM-Kepegawaian	3
SIM-WP	3
SIM-Pajak	3
Web Server	4
Data User dan Password	3

Gambar.4

tentang matrik resiko akan didapatkan hasil level resiko. Hasil perhitungan dan level resiko terlihat pada gambar 5.

No	Aset	Nilai Aset	Nilai Ancaman	BIA	Nilai Resiko	Level Resiko
1	PC	5	0	1	0	low
2	Server	12	0	4	0	low
3	Jaringan Fisik Kabel	8	0	2	0	low
4	Kamera CCTV	6	0	1	0	low
5	DVDR CCTV	6	0	1	0	low
6	Cisco Router	9	0	3	0	low
7	ESPT	9	0.13	2	2.34	med
8	EFAKTUT	9	0.13	2	2.34	med
9	EFILLING	8	0.1	2	1.6	low
10	EBILLING	7	0.08	2	1.12	low
11	SIM-Kepegawaian	6	0.03	3	0.54	low
12	SIM-WP	7	0.13	3	2.73	med
13	SIM-Pajak	9	0.1	3	2.7	med
14	Web Server	10	0.02	4	0.8	low
15	Data User dan Password	10	0.13	3	3.9	high

Gambar 5

Dari tabel 10 didapatkan aset yang memiliki resiko tinggi dan diperlukan kontrol keamanan untuk mengurangi resiko yang terjadi adalah Data User dan Password dengan prosentase 6,67% dari data Aset yang terdaftar, 26,67% memiliki level Medium serta 66,67 memiliki level High.[2]

5. Kesimpulan

Dari hasil penelitian yang telah dilakukan dapat disimpulkan bahwa dari aset yang terdaftar hanya satu aset yang memiliki resiko High yaitu Data Username dan Password dengan prosentase 6,67%. Untuk meningkatkan kualitas penelitian diperlukan analisa yang lebih banyak dari jenis kejadian,sehingga hasil analisanya lebih mendalam. Rekomendasi lainya yaitu penelitian dapat dilanjutkan kepada pemilihan kontrol keamanan dalam rangka menyusun portofolio SMKI.[2]

6. Referensi

[1] R. Budiarto, "Penerapan Metode FMEA Untuk Keamanan sistem Informasi," *Semin. Nas. IPTEK Ter.*, vol. 1, pp. 73–78, 2017.

[2] I. Santosa and D. Kuswanto, "Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ," *Rekayasa*, vol. 9, no. 2, p. 108, 2016.

[3] Raden Budiarto, "Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode Fmea Dan Iso 27001 Pada Organisasi Xyz," *J. Comput. Eng. Syst. Sci.*, vol. 2, no. 2, pp. 48–58, 2017.