Journal on Education
Volume 05, No. 02, Januari-Februari 2023, pp. 3437-3443
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

Analisis Manajemen Resiko Keamanan Informasi pada Kantor Dinas Pendidikan Gunung Tua

Lili Saputri[1], Mirna Annifah Hsb[2], Tursina Juliani[3], Muhammad Dedi Irawan[4]
[1, 2, 3, 4]Universitas Islam Negeri Sumatera Utara, Jl. William Iskandar Ps. V, Deli Serdang, Sumatera Utara
Lilisaputri890@gmail.com

Abstract

Implementation of Information Technology in government institutions is currently needed to facilitate data collection and strategic decision making. The Tax Service Office is one of the government agencies engaged in education. The Education Office is a government agency located in the Gunung Tua Regency Government Office Complex, in its services such as processing data from each school, which is in Pesawaran Regency which can be used in processing certification data. Information technology analysis is carried out to ensure the operational continuity used by the service, whether the existing information technology is used as well as possible, because if it is not used properly it will cause some problems or existing losses such as data loss, or errors. data use, computer abuse, inaccurate information, because in this system the data is confidential and sensitive. For this reason, an Information Security Management System (ISMS) is needed in managing its security. In implementing ISO 27001 previously required information security risk management. This risk management activity is needed to determine the Control Objectives that will be taken to handle risks that might occur. In implementing risk management, results were obtained only for username and password level assets that had a high risk (6.67%) of the 15 assets that had been registered, so that security controls related to usernames and passwords were needed to minimize or reduce risk.
Keywords: Risk Management, Education Office, SMKI

Abstrak

ImplementasiTeknologi 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 Pendidikan. Dinas Pendidikan merupakan dinas pemerintahan yang terdapat pada Komplek Perkantoran Pemkab Gunung Tua, dalam pelayanan nya seperti pengolahan data dari masing-masing sekolah, yang ada pada Kabupaten Pesawaran yang dapat di gunakan dalam pengolahan data sertifikasi. Analisis teknologi informasi di lakukan untuk menjamin keberlanjutan operasional yang digunakan oleh dinas apakah teknologi informasi yang ada sudah di gunakan dengan sebaik-baik nya, karena jika dalam pemanfaatan tidak digunakaan dengan tepat maka akan menimbulkan beberapa permasalahan atau kerugian yang ada seperti kehilangan data, atau penyalah gunaan data, penyalah gunaan komputer, informasi yang tidak akurat, karena pada sistem ini data yang ada sifatnya rahasia dan sensitif. 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, Dinas Pendidikan, SMKI

Corresponding author Lili Saputri
Email Address: Lilisaputri890@gmail.com (Fakultas Sistem Informasi, Sains Dan Teknologi Universitas Islam Negeri Sumatera Utara, Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Deli Serdang, Sumatera Utara)
Received 08 January 2023, Accepted 19 January 2023, Published 19 January 2023

PENDAHULUAN

Keamanan informasi elektronik jadi perihal yang amat berarti di industri fasilitator pelayanan teknologi data (TI) ataupun pabrik yang lain, semacam: industri exportimport, transportasi, badan finansial, pebelajaran, pemberitaan, sampai perbankan yang memakai sarana TI serta menempatkannya

selaku prasarana kritikal (berarti). Data ataupun informasi merupakan aset untuk industri. Keamanan informasi dengan cara tidak langsung bisa membenarkan kelangsungan bidang usaha, kurangi efek, memaksimalkan return on investment serta mencari peluang bidang usaha. Terus menjadi banyak data industri yang ditaruh, diatur serta disharing hingga terus menjadi besar pula efek terbentuknya kehancuran, kehabisan ataupun terekspos nya informasi ke pihak eksternal yang tidak di idamkan. Gimana informasi ataupun data itu diatur, dipelihara serta diekspose, melatarbelakangi disusunnya ISO17799, standar buat system manajemen keamanan data.

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).

Keamanan Informasi

Dikala penguasa serta golongan pabrik mulai mengetahui keinginan buat mengamankan pangkal energi data mereka, atensi hampir terfokus dengan cara khusus pada perlindunga peranti keras informasi hingga sebutan keamanan sistem dipakai. Sebutan keamanan sistem dipakai buat mengambarkan perlindungna bagus perlengkapan pc serta nonkomputer, sarana, informasi serta data dari penyalahgunaan pihak- pihak yang tidak berhak.

Tujuan Keamanan Informasi

1. Keamanan informasi ditujuakan untuk mencapai tiga tujuan utama yakni:
   Kerahasiaan. Perusahaan berusaha untuk melindungi data dan informasinya dari pengungkapan orang-orang yang tidak berwenang.
2. 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.

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.

Manajemen Keamanan Informasi

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

1. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
2. Mendefenisikan risiko yang dapat disebabkan oleh ancaman-ancaman tersebut
3. Menentukan kebijakan keamanan informasi
4. 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.[3]

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.

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:

1. 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.

METODE

Pada ulasan ini hendak dipaparkan metodologi dalam riset ini mulai dari pengumpulan informasi buat melaksanakan pengenalan peninggalan, melaksanakan kalkulasi Angka peninggalan yang sudah dikumpuklan, melaksanakan pengenalan bahaya serta kelemahan peninggalan, melaksanakan analisa akibat bidang usaha ataupun yang kerap diucap Business Impact Analysis(BIA), melaksanakan pengenalan tingkat efek serta yang terakhir membagi risk value buat mengenali tingkat efek dari peninggalan.

Langkah dini riset ini merupakan mengakulasi informasi asset ialah peninggalan yang memiliki informasi serta ataupun data. Pengenalan Peninggalan dicoba buat memastikan asset yang berkaitan dengan control akses di KPP Biro Pendidikam Sehabis peninggalan teridentifikasi, tahap berikutnya ialah melaksanakan kalkulasi angka peninggalan. Pendekatan yang dicoba dengan memakai 3 pandangan 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.

HASIL DAN DISKUSI

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

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.

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

Langkah selanjutnya yaitu menghitung Nilai Resiko dari NA, BIA dan NT yang sudah didapatkan tentang matrik resiko akan didapatkan hasil level resiko. Hasil perhitungan dan level resiko terlihat pada 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.

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

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 dilanjutka kepada pemilihan kontrol keamanan dalam rangka menyusun portofolio SMKI.

REFERENSI

D. Setiawan och M. P. Halilintar, "Analisis Gangguan Sambaran Petir Terhadap Kerusakan Perangkat IT Pusat Komputer Universitas Lancang Kuning Menggunakan Metode Collection Volume," Pekanbaru, 2015.

M. Utomo, A. H. N. Ali och I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," JURNAL TEKNIK ITS, vol. 1, nr 1, pp. A288-A293, 2012

I. iSantosa iand iD. iKuswanto, i"Analisa iManajemen iResiko iKeamanan iInformasi ipada Kantor iPelayanan iPajak iPratama iXYZ," i*Rekayasa*, ivol. i9, ino. i2, ip. i108, i2016.

B.Mahersmi,F.A. Muqtadiroh dan B.C. Hidayanto, "Analisis Risiko Keamanan Informasi dengan Menggunakan Metode Octave dan Kontrol Iso 27001 PadaDishubkominfo KabupatenTulungagung,"dalam Seminar Sistem Informasi Indonesia,Surabaya,2016.

I. Desy, B. C. Hidayanto dan H. Maria Astuti, "penilaian Risiko Keamanan informasi menggunakan metode failure mode and effects analysis di divisi TI pt. bank Xyz surabaya, "dalam seminar nasional sistem informasi Indonesia, Surabaya, 2014.