KOMPOSISI RESIKO KEAMANAN TEKNOLOGI INFORMASI DITINJAU DARI SISI TEKNOLOGI DAN SUMBER DAYA MANUSIA

Sony Susanto
ssony462001@yahoo.com

ABSTRAK

Pada era teknologi informasi saat ini, kita ketahui bahwa pengolahan informasi merupakan hal yang sangat penting. Persaingan bisnis pada era ini telah melibatkan teknologi informasi dalam mengelola informasinya untuk meningkatkan daya saing dalam bisnisnya oleh semua perusahaan terutama perusahaan besar.

Faktor teknologi merupakan komponen utama dalam mengelola system informasi terutama mengenai keamanan pada teknologi informasi tersebut. Karena itu maka perlu diadakan analisa resiko keamanan berdasarkan teknologi untuk mengurangi resiko keamanan pada system informasinya.

Selain faktor teknologi faktor sumber daya manusia merupakan sumber dari keamanan informasi yang sangat penting untuk dianalisa dan dilakukan perbaikan jika ada kelemahan sehingga dapat mengurangi resiko dalam keamanan informasi.

Dilaporkan bahwa terjadi *network incident* pada bulan Maret sejumlah 4850 dan bulan april pada tahun yang sama (2013) sejumlah 2032 jadi total laporan terjadinya *network incident* menjadi 6882 (ID-CERT 2013).

Keyword : analisa, resiko, keamanan, teknologi, informasi.

I. PENDAHULUAN

Fokus penelitian ini adalah manajemen resiko keamanan. Ruang lingkupnya "analisa resiko keamanan pada jaringan teknologi informasi ditinjau dari teknologi dan sumber daya manusia difokuskan pada simpeg di pemkot Sukabumi" . Studi kasus dilakukan di sistem informasi kepegawaian di Pemkot Sukabumi.

1.1 Identikasi Masalah

Rumusan Masalah

Dalam penyusunan jurnal ini, akan dilakukan perumusan masalah, pembahasan dan penyajian yang berkaitan dengan resiko keamanan pada jaringan teknologi informasi khususnya mengenai resiko-resiko yang berkaitan dengan keamanan jaringan teknologi informasi yang terdiri dari : Resiko-resiko keamanan pada teknologi informasi, sistem keamanan dan teknologi keamanan, Masalah keamanan dan solusinya ditinjau secara holistik dari aspek teknologi.

Tujuan Penelitian

Tujuan utama penelitian ini adalah untuk mengidentifikasi dan mengkonsolidasikan resiko keamanan pada jaringan teknologi informasi, dan memformulasikan suatu methodologi analisa serta mengkategorisasikan resiko-resikonya. Manfaat yang didapat pada penelitian ini adalah penelitian ini akan membentuk suatu formula untuk mendesign sistem yang aman, dalam bentuk framework yang terstruktur untuk menganalisa resiko. Penelitian ini khusus pada studi kasus dilakukan pada simpeg (sistem informasi kepegawaian).

1.2 Metode yang Digunakan

1.2.1 Studi literatur

Pada jurnal ini dilakukan studi literatur baik itu pada buku-buku, majalah-majalah, jurnal-jurnal maupun *surfing* internet.

1.2.2 Wawancara

Pada pengumpulan data atau informasi dilakukan pula wawancara dengan orang yang ahli pada bidangnya terutama mengenai teknologi informasi dan resikonya. Serta dilakukan wawancara untuk melakukan pengisian kuesioner

pada awal kuisioner itu diberikan untuk diisi di lingkungan bagian simpeg di Badan Kepegawaian dan Diklat Pemkot Bandung.

1.2.3 Studi kasus

Pada jurnal ini dilakukan pula studi kasus pada suatu organisasi sebagai strategi untuk menganalisa keamanan suatu jaringan teknologi informasi terhadap organisasi tersebut yang hasilnya sebagai masukan kepada pihak manjemen untuk dasar pengambilan keputusanya dalam mengangani masalah teknologi informasi sebagai pendukung proses bisnisnya. Studi kasus ini dilakukan di sistem informasi kepegawaian di Badan kepegawaian dan Diklat Pemkot Sukabumi.

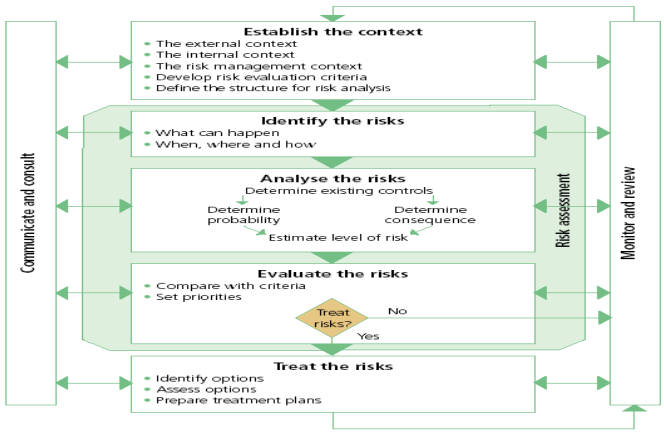
II. LANDASAN TEORI

2.1. Proses Manajemen Resiko

Resiko didefinisikan sebagai posibilitas terjadinya sesuatu yang dapat berdampak pada tujuan. Resiko diukur menggunakan konsekuensi dan *likelihood*. Manajemen resiko merupakan suatu proses berulang dari langkah-langkah yang sudah terdefinisi dengan baik secara berurutan dengan mengkontribusikan resiko dan dampaknya (OB/7, 1999)

2.2. Framework Manajemen Resiko berdasarkan Standar Australia

Pada penelitian ini standar yang dipakai adalah Standar Australia/New Zealand (AS/NZS 4360:1999) untuk manajemen resikonya. Adapun elemen utama dari standar ini adalah sebagai berikut :



Gambar 1. Proses Manajemen Resiko (OB/7, 1999).

Gambar 1 tersebut merupakan proses manajemen resiko yang berdasarkan Standar Australia (OB/7, 1999) yang gunanya sebagai panduan langkah-langkah dalam menentukan resiko-resiko yang harus diidentifikasi serta dianalisa dan dievaluasi sehingga dapat dikelola resiko-resiko tersebut.

2.3. Pengaruh resiko keamanan terhadap resiko bisnis

Grup Gartner (Witty, et al..2001) menyarankan bahwa resiko dapat diukur dampaknya atas jenis kerugian sebagai berikut : Finansial, Keuntungan kompetitif, Legal atau regulator, Operasional atau layanan dan Reputasi market.

2.4. Pelanggaran Keamanan

Dilaporkan bahwa pada tahun 2008 terjadi serangan DoS (*Denial of Service*) sebesar 21% dari responden yang mengalami serangan sistem keamanan komputernya (CSI, 2008).Selain itu terjadi peningkatan serangan terhadap keamanan teknologi informasi pada jenis serangan *unauthorized access* sebesar 4% yang asalnya 25% tahun 2007 dan meningkat menjadi 29% tahun 2008 (CSI, 2008).

2.5.Teknologi Informasi dan Sistem Informasi

Komputer merupakan bentuk teknologi informasi pertama (cikal bakal) yang dapat melakukan proses pengolahan data menjadi informasi. Dalam kurun waktu yang kurang lebih sama, kemajuan teknologi telekomunikasi terlihat sedemikian pesatnya, sehingga telah mampu membuat dunia menjadi terasa lebih kecil (mereduksi ruang dan waktu = *time and space*). Dari sejarah ini dapat disimpulkan bahwa yang dimaksud dengan teknologi informasi adalah suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data/informasi tersebut dalam batas-batas ruang dan waktu (Indrajit,2002).

Definisi keamanan sistem informasi menurut ITS (badan standard di Swedia) adalah "Keamanan dalam sistem informasi yang meliputi baik manual maupun otomatis"

2.6. Keamanan Komponen Jaringan Teknologi Informasi

Definisi keamanan teknologi informasi menurut ITS (badan standard di swedia) adalah "Keamanan dalam system teknologi informasi yang meliputi keamanan ADP *(Automatic Data Processing)* dan keamanan komunikasi". Sedangkan definisi keamanan sistem komputer menurut Gollman adalah "Berkaitan dengan teknik yang dilakukan untuk memelihara keamanan dalam sistem komputer"

III. STUDI KASUS ANALISA KEAMANAN TEKNOLOGI INFORMASI DITINJAU DARI SISI SUMBER DAYA MANUSIA DI BADAN KEPEGAWAIAN DIKLAT PEMERINTAH KOTA SUKABUMI

Pada studi kasus ini peneliti menggunakan pendekatan *risk assessment* untuk menganalisa keamanan teknologi informasi dari simpeg ini dengan *framework* yang telah dijelaskan sebelumnya. Sedangkan penjelasan lengkap

mengenai bagaimana dan hasil dari penelitian ini dapat dilihat pada bagian di bawah ini.

3.1. Metodologi Analisa Resiko

Metodologi yang digunakan pada studi kasus ini berdasarkan Standar Australia. Alasan digunakan Standar Australia pada studi kasus ini karena standar ini sudah matang dan sudah digunakan di seluruh dunia. Pada dunia bisnis dikenal dengan level resiko bisnis yang merupakan hasil dari *vulnerability*. Adapun formula untuk mentranslate dari *vulnerabilty* teknik terhadap level resiko bisnis itu adalah sebagai berikut:

Residual Risk = (Impak dari Inherent Risk) X Peluang (Vulnerabilities – Countermeasure)

Keterangan:

Residual Risk : Merupakan tingkat keseriusan setiap resiko.
Impak dari *Inherent Risk* : Merupakan tingkat negatif pada objek bisnis dimana skenario resiko itu terjadi.

Peluang : Merupakan peluang terjadinya resiko terbagi menjadi dua yaitu :

a. *Vulnerability* : Merupakan kelemahan sistem yang ada dan dapat menimbulkan resiko dari anacaman terhadap sistem itu.
b. Countermeasure : Merupakan kontrol yang dapat memberi efek untuk memitigasi terhadap resiko inherent. Ini bisa berbentuk dalam teknik, prosedur, manual atau otomatis.

Berdasarkan Standard Australia AS/NZS 4360 : 1999, bahwa impak, *vulnerability* dan residual risk dapat didefinisikan sebagai berikut :

3.2. Ukuran Kualitatif Konsekuen atau Impak

Impak : Tingkat dampak jika terjadi eksploitasi pada *vulnerability*.

a. T (impak tinggi) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan pada opersional atau keuangan atau memalukan organisasi.
b. S (impak sedang) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan atau *unavailability (denial of service)* pada system internal.
c. R (impak rendah) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan terbukanya informasi tentang sistem dan struktur jaringan internal.

3.3. Ukuran Kualitatif Peluang

Peluang : Merupakan peluang terjadinya suatu resiko.

a. T (peluang tinggi) : Dimana *vulnerability* diketahui dengan baik, dapat dieksploitasi dengan tool-tool dan teknik-teknik yang tersedia di internet, serta hanya memerlukan pengalaman dan pengetahuan yang sedikit.
b. S (peluang sedang) : Dimana vulnerabilty tidak langsung nyata teridentifikasi, tapi memerlukan penelitian, ketekunan, serta pembiasaan penggunaan teknik dan tool.
c. R (peluang rendah) : Dimana *vulnerability* diidentifikasi memerlukan tingkat pengetahuan dan teknik yang tinggi dan teknik serta *tool* yang tak tersedia di umum.

3.4. Residual Risk

Residual Risk : Tingkat keseriusan resiko terhadap bisnis organisasi.

a. T (resiko tinggi) : Dimana isu harus segera dilakukan pencegahan efek negatif pada objek bisnis.

b. S (resiko sedang) : Dimana isu harus dengan cepat dilakukan pengurangan terhadap resiko.
c. R (resiko rendah) : Dimana isu harus dengan segera meningkatkan keamanan.

Tabel 1 Analisa resiko kualitatif – tingkat resiko (OB/7, 1999)

Konsekuen	Peluang		
	Rendah	Sedang	Tinggi
Tinggi	S	T	T
Sedang	R	S	T
Rendah	R	R	S

Keterangan :

R : Resiko rendah

S : Resiko sedang

T : Resiko tinggi

3.5. Kategorisasi Resiko

Kategorisasi resiko ini dilakukan berdasarkan tujuh prinsip keamanan yaitu :

a. *Intrusion* : Menjamin bahwa akses terhadap sistem dan informasi hanya dapat dilakukan melalui metode akses yang terotorisasi.
b. *Authentication* : Menjamin bahwa hanya orang yang terotorisasi yang dapat mengakses sistem dan informasi.
c. *Authorization* : Menjamin bahwa akses terhadap sistem dan informasi sesuai dengan otorisasi yang diberikan pada user.
d. *Encryption* : Proteksi informasi sehingga terlindungi ketika informasi itu di kirim dan disimpan pada storage.
e. *Accountability* : Menjamin bahwa akses terhadap sistem dan informasi oleh user tercatat secara benar.

f. *Availability* : Menjamin bahwa sistem dan informasi tersedia ketika diperlukan oleh user yang berhak.
g. *Endurability* : Menjamin bahwa resiko keamanan dipelihara sesuai pada level yang dapat diterima sepanjang waktu.

3.6. Hasil penelitian

Setelah dilakukan penelitian dan evaluasi simpeg di Badan Kepegawaian dan Diklat Pemerintah Kota Sukabumi maka laporan hasil penelitian dan analisanya adalah sebagai berikut :

Tabel 2 Hasil Penelitian

No	Komponen Resiko	Peluang	Impak	Residual Risk	Penyebab Resiko	Solusi
		T/S/R	T/S/R	T/R/S	O/U/I/N	P/T
1	Intrusion	T	T	T	U	T
2	Authentication	R	T	S	I	T
3	Authorization	R	S	S	I	P
4	Encryption	S	T	T	U	P
5	Accountability	S	T	T	U	P
6	Availability	T	T	T	O	P
7	Endurability	R	R	R	N	T

3.6.1. Penjelasan Pengisian Kuesiomer

1. Peluang : Merupakan peluang terjadinya suatu resiko.
   a. T (peluang tinggi) : Dimana *vulnerability* diketahui dengan baik, dapat dieksploitasi dengan tool-tool dan teknik-teknik yang tersedia di internet, serta hanya memerlukan pengalaman dan pengetahuan yang sedikit.
   b. S (peluang sedang) : Dimana *vulnerabilty* tidak langsung nyata teridentifikasi, tapi memerlukan penelitian, ketekunan, serta pembiasaan penggunaan teknik dan tool.

c. R (peluang rendah) : Dimana *vulnerability* diidentifikasi memerlukan tingkat pengetahuan dan teknik yang tinggi dan teknik serta tool yang tak tersedia di umum.

2. Impak : Tingkat dampak jika terjadi eksploitasi pada *vulnerability*.
   a. T (impak tinggi) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan pada opersional atau keuangan atau memalukan organisasi.
   b. S (impak sedang) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan atau *unavailability* (*denial of service*) pada system internal.
   c. R (impak rendah) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan terbukanya informasi tentang sistem dan struktur jaringan internal.

3. Residual Risk : Tingkat keseriusan resiko terhadap bisnis organisasi.
   a. T (resiko tinggi) : Dimana isu harus segera dilakukan pencegahan efek negatif pada objek bisnis.
   b. S (resiko sedang) : Dimana isu harus dengan cepat dilakukan pengurangan terhadap resiko.
   c. R (resiko rendah) : Dimana isu harus dengan segera meningkatkan keamanan.

Tabel 3 Analisa residual resiko kualitatif – tingkat resiko (OB/7, 1999)

Konsekuen	Peluang		
	Rendah	Sedang	Tinggi
Tinggi	S	T	T
Sedang	R	S	T
Rendah	R	R	S

Keterangan :

R : Resiko rendah

S : Resiko sedang

T : Resiko tinggi

3.6.2. Penyebab Resiko Dan Solusi:

Penyebab Resiko : Merupakan bentuk tindakan yang kurang dalam masalah keamanan sehingga bisa menimbulkan terjadinya resiko keamanan.

a. O (*oversight*) : Klien sadar adanya resiko tapi tak ada tindakan *countermeasure-nya*.
b. U (*unawareness*) : Klien tak menyadari adanya resiko sehingga tidak ada tindakan untuk menangani resiko itu.
c. I (*inadequacy*) : Klien sadar adanya resiko dan melakukan tindakan dalam menangani resiko tetapi rencana *countermeasure*-nya tak memadai.
d. N (*not available*) : Klien sadar betul adanya resiko dan melakukan *countermeasure*-nya secara tepat.

Tabel 4 Jumlah Penyebab Resiko Dan Solusinya

No	Penyebab Resiko	Jumlah	Keterangan
1	O (*oversight*)	1	Lakukan *countermeasure*
2	U (*unawareness*)	3	Lakukan pelatihan keamanan
3	I (*inadequacy*)	2	Lakukan *countermeasure* yang memadai
4	N (*not available*)	1	Tak ada

3.6.3. Solusi

Merupakan pemecahan masalah terhadap resiko keamanan teknologi informasi yang terbagi menjadi tiga kelompok yaitu :

a. Personal (P) : Dimana resiko dapat dimitigasi dengan managemen perubahan dan pelatihan terhadap karyawan.
b. Teknologi (T) : Dimana resiko dapat dimitigasi dengan menggunakan solusi teknologi yang tepat

Dari tabel penelitian di atas maka untuk mengetahui komposisi keadaan keamanan teknologi informasi di badan diklat ini maka untuk penyebab dan solusi dimatrikan sehingga dapat terlihat komposisinya seperti di tabel 2.

3.6.4. Komposisi keamanan teknologi informasi

Jadi komposisi keamanan teknologi simpeg di kantor Badan Kepegawaian dan Diklat Pemerintah Kota Sukabumi dapat dilihat dalam di tabel 5 seperti di bawah ini.

Tabel 5 Komposisi Penyebab Dan Solusi Resiko Keamanan Sistem Informasi Pegawai

Penyebab Resiko	Solusi		Jumlah Penyebab (persentase)
	Personal	Teknologi	
O (*oversight*)	1	0	1(14%)
U (*unawareness*)	2	1	3(43%)
I (*inadequacy*)	1	1	2(29%)
N (*not available*)	0	1	1(14%)
Jumlah Solusi (persentase)	4(57%)	3(43%)	7(100%)

Jadi keadaan teknologi informasi di Kantor Badan Kepegawaian dan Diklat Pemkot Sukabumi maka masalah terbesar adalah *unwareness* yaitu 43% dan solusi yang dominan dengan personal yaitu 57%.

IV. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa:

a. Formula yang diajukan pada penelitian ini merupakan suatu metodologi untuk menganalisa serta mengkategorisasikan resiko keamanan pada jaringan teknologi informasi ditinjau dari sisi teknologi dapat diterapkan pada kehidupan sehari-hari.
b. Metode analisa ini dapat membantu menganalisa keamanan jaringan teknologi informasi dengan fokus pada penyebab dan solusi untuk jaringan teknologi informasi yang kritis pada suatu organisasi.
c. Metode analisa ini dapat membantu para perancang jaringan teknologi informasi untuk membangun jaringan teknologi informasi yang aman.

4.2. Saran

Dari penelitian ini maka disarankan bahwa :

a. Penelitian ini ditujukan pada organisasi teknologi informasi secara umum maka untuk mereka yang ingin menggunakan metode analisa ini dapat digunakan terhadap berbagai jenis teknologi informasi yang bersifat khusus seperti data warehousing dengan melakukan pengadaptasian terhadap objek yang diteliti.
b. Karena penelitian ini dilakukan pada hanya satu studi kasus maka para peneliti yang ingin menggunakan metode ini sebaiknya di teliti pada multi studi kasus sehingga ada perkembangan pada dunia pengetahuan.

REFERENSI

Alan Sugano, 2004, The Real-World Network Troubleshooting Manual, Charles River Media, Inc.

Ankit Fadia, 2003, Network Security : A Hacker's Perspective, Macmillan India Ltd.

AusCERT, 2000, Information Security Standard, URL : http/www/anscert.org.au/Information/standards.html.

Beny Benardi, 2004 , Membangun Firewall dengan Cisco Router, PT Bex Media Komputindo.

Budi Rahardjo, 2005, Keamanan Sistem Informasi Berbasis Internet, Versi 5.4, PT Insan Infonesia-Bandung & PT INDICISC-Jakarta.

Carl Roper, Joseph Grau, and Lynn Fischer, 2006, Security Education, Awareness, and Ttraining, From Theory to Practice, Elsevier Inc.

Chris McNab, 2004, Network Security Assessment, O'Reilly.

David Kosiur, Uderstanding Electronic Commerce, Microsoft Press.

Depkominfo, 2007, Blue Print Aplikasi E-Government Pemerintah Pusat, Depkominfo.

Deris Setiawan, 2005, Sistem Keamanan Komputer, PT Elex Media Komputindo.

Didik Subyantara, 2004, Instalasi dan konfigurasi Jaringan Microsoft Windows, PT Elex Media Komputindo.

Parag Diwan, 2002, Information System Management, Golden Books Sdn, Bhd.

Patrick T. Campbell, 1996, Jaringan di Kantor Kecil, PT Elex Media Komputindo.

R. Eko Indrajit, 2005, Manajemen Sistem Informasi dan Teknologi Informasi, E-book Perbanas.

Ridwan Sanjaya ..dkk, 2005, Administrasi Jaringan Komputer Lintas Platform, PT Elex Media Komputindo.

Rinaldi Munir, 2006, Kriptografi, Informatika.

Robert Richahardson, 2008, Computer crime & security survey, CSI.

Rolf Oppliger, 2002, Internet and Intranet Security, Artech House, Inc.

Ron Ben Natan, 2005, Implementing Database Security and Auditing, Elsevier Digital Press.

S'to, 2009, CEH : 100% illegal, Jasakom.

Straub, D.W. and Welke, RJ, 1998,Coping with system risk: security planning models for management decision, MIS Quarterly, Minneapolis.

Stuart McClure, Saumil Shah, and Shreeraj Shah, 2003, Web Hacking Serangan dan Pertahanan, ANDI.

Thomas R. Peltier, 2005, Information Security Risk Analysis, Second Edition, Auerbach Publications, Taylor & Francis Group.

Tutang dan Kodarsyah, 2002, Belajar Jaringan Sendiri, Medikom Pustaka Mandiri.

Wesley J. Noonan, 2004, Hardening Network Infrastructure, The McGraw-Hill Companies, Inc.

Yin, R.K, 1993, Application of case study reserch, Sage.

[Yin, R.K, 1994, Case study reserch-design and methods, Sage.

Zikmund, W.G, 1997, Businees reserch methods, The Dryden Press.