Standar Sistem Manajemen Keamanan Informasi Menggunakan ISO 27001

Ilham Eka Putra

Jurusan Sistem Komputer, Universitas Sriwijaya

Ilhamekaputra23@gmail.com

Abstrak

Manajemen keamanan informasi sangat penting untuk digunakan, terutama bagi instansi pendidikan, dikarenakan mampu mengurangi resiko ancaman terhadap penggunaan teknologi informasi bagi organisasi pendidikan. Manajemen keamanan informasi sangat diperlukan sebagai upaya untuk meminimalkan resiko dalam meningkatnya ancaman data dan informasi. Pelaksanaan manajemen keamanan informasi dimaksudkan untuk mengetahui masalah teknis dan masalah non teknis. Penelitian ini menggunakan standard ISO 27001:2005, dikarenakan standard ISO 27001:2005 dapat menyesuaikan dengan instrumen penelitian pada kebutuhan organisasi yang dikembangkan dan fokus pada manajemen keamanan informasi. Hasil penelitian menggunakan standard ISO 27001:2005 adalah dapat mengurangi resiko tingkat keamanan, dan dapat melakukan evaluasi secara berkesinambungan, serta meningkatkan control keamanan yang direkomendasikan pada institusi XYZ.

Kata Kunci Standard ISO 27001:2005, Manajemen Keamanan Informasi, IT Support.

Abstrack

Information security management is very important to use, especially for educational instutions, because it is able to reduce the risk of threats to the use of information technology for educational organizations. Information security management is indispensable as an effort to minimize the risk of data enhancement and information threats. Implementation of information security management is intended to know technical problems and non-technical problems. The research uses the ISO 27001:2005 standard, as the ISO 27001:2005 standard can adapt to research instruments on the needs of the developed organization and focus on information management. The results of the research using the ISO 27001:2005 standard are able to reduce the risk of security level, and can evaluate continuously, and improve the security control recommended by XYZ institutions.

Keywords – ISO 27001:2005 Standard, Information Security Management, IT Support.

I. Pendahuluan

Keamanan data menjadi hal yang penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, transportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatnya sebagai infrastruktur penting.

Informasi adalah aset 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 terekspos nya data ke pihak eksternal yang tidak diinginkan.

II. Pembahasan

2.1. Apa itu keamanan Informasi?

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 diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

Gambar 2.1 Elemen-elemen keamanan informasi

2.2. Ancaman Terhadap Sistem Informasi

Ancaman adalah suatu aksi atau kejadian yang dapat merugikan perusahaan. Kerugian bisa berupa uang, tenaga, kemungkinan berbisnis (*business opportunity*), reputasi organisasi bahkan mungkin dapat menyebabkan pailit. Menurut W. Stallings ada beberapa kemungkinan ancaman, yaitu:

1) *Interruption*, perangkat sistem rusak atau menjadi tidak tersedia, merupakan ancaman terhadap aspek *availability* (ketersediaan).
2) *Interception*, pengaksesan informasi oleh pihak yang tidak berwenang.
3) *Modification*, pihak yang tidak memiliki wewenang tidak hanya mengakses informasi tetapi juga melakukan perubahan terhadap informasi.
4) *Fabrication*, penyisipan objek palsu ke dalam sistem oleh pihak yang tidak berwenang.

Berikut ini beberapa kasus yang berhubungan dengan ancaman terhadap keamanan sistem informasi di Indonesia antara lain:

1. Pada Januari 2000, beberapa sistus web di Indonesia diacak-acak oleh cracker yang menamakan dirinya"fabianclone" dan "aisenodni" (Indonesia dibalik). Situs yang diserang

termasuk Bursa Efek Jakarta, BCA, Indosatnet, dan beberapa situs besar lain yang tidak dilaporkan.

2. September dan Oktober 2000, setelah membobol Bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali.
3. 16 April 2001, Polda DIY meringkus seorang *carder* (pembobol kartu kredit). Tersangka diringkus di Bantul dengan barang bukti sebuah paket berisi lukisan berharga 30 juta rupiah.
4. Dikutip dari berita elektronik www.republika.co.id, perubahan kartu tanda penduduk (KTP) menjadi bentuk elektronik (e-KTP), merupakan salah satu contoh sistem yang rentan dalam hal keamanannya, mengingat data yang ada di dalamnya merupakan data rahasia, data privasi yang perlu dilindungi.

Menurut David Icove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi 4, yaitu:

1) Keamanan yang bersifat fisik (*physical security*).
2) Keamanan yang berhubungan dengan orang.
3) Keamanan dari data dan media serta teknik komunikasi.
4) Keamanan dalam operasi.

2.3. Standar Manajemen Keamanan Informasi (SMKI)

Pengelolaan keamanan sistem informasi yang baik dibutuhkan untuk mengantisipasi ancaman-ancaman yang mungkin terjadi. Bagaimana perusahaan dapat menerapkan dan mengelola keamanan sistem informasi, melatarbelakangi disusunnya seri ISO/IEC 27000, merupakan standar tentang *Information Security Management System* (ISMS) atau dikenal juga dengan istilah Sistem Manajemen Keamanan Informasi (SMKI). Menurut ISO/IEC 27000:2014, ISMS adalah pendekatan sistematis untuk menetapkan, mengimplementasi, operasional, pemantauan, peninjauan, pemeliharaan dan meningkatkan keamanan informasi pada organisasi untuk mencapai tujuan bisnis. Menurut ISO/IEC 27001:2014, keamanan sistem informasi tidak hanya berhubungan dengan penggunaan perangkat lunak antivirus, *firewall*, penggunaan *password* untuk komputer, tetapi merupakan pendekatan secara keseluruhan baik dari sisi orang, proses dan teknologi untuk memastikan berjalannya efektivitas keamanan. *International Organization for Standardization* (ISO) adalah sebuah organisasi internasional non-pemerintahan untuk standarisasi. *Internasional Electrotechnical Commission* (IEC) adalah suatu oraganisasi standarisasi internasional yang menyiapkan dan mempublikasikan standar internasional untuk semua teknologi elektrik, elektronika dan teknologi lain yang terkait, yang dikenal dengan elektroteknologi. Standarisasi di gunakan untuk mendukung inovasi dan memberikan solusi untuk tantangan global. Seri ISO/IEC 27000 merupakan pembaharuan dari ISO 17799. ISO/IEC 27001:2005 telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) untuk SMKI.

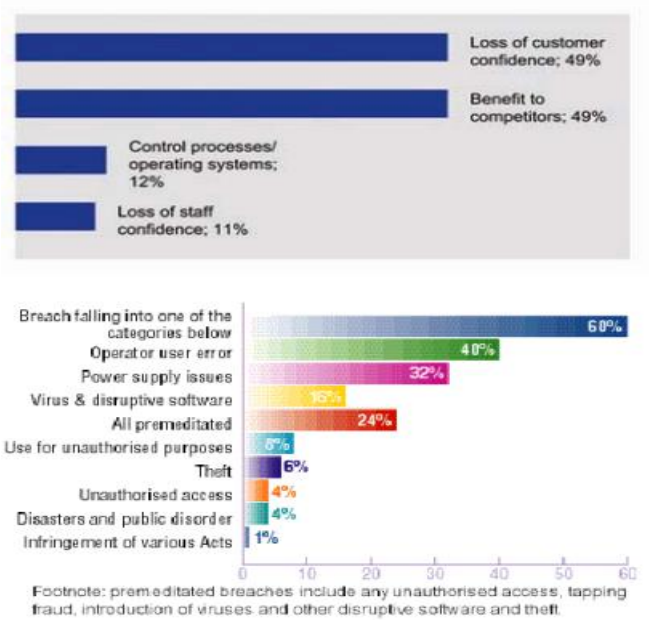
Seri ISO/IEC 27000 terdiri dari :

- ISO/IEC 27000:2009 - ISMS Overview and Vocabulary
- ISO/IEC 27001:2005 - ISMS Requirements
- ISO/IEC 27002:2005 - Code of Practice for ISMS
- ISO/IEC 27003:2010 - ISMS Implementation Guidance
- ISO/IEC 27004:2009 - ISMS Measurements
- ISO/IEC 27005:2008 - Information Security Risk Management
- ISO/IEC 27006:2007 - ISMS Certification Body Requirements
- ISO/IEC 27007 - Guidelines for ISMS Auditing

2.4. Mengapa diperlukan keamanan informasi?

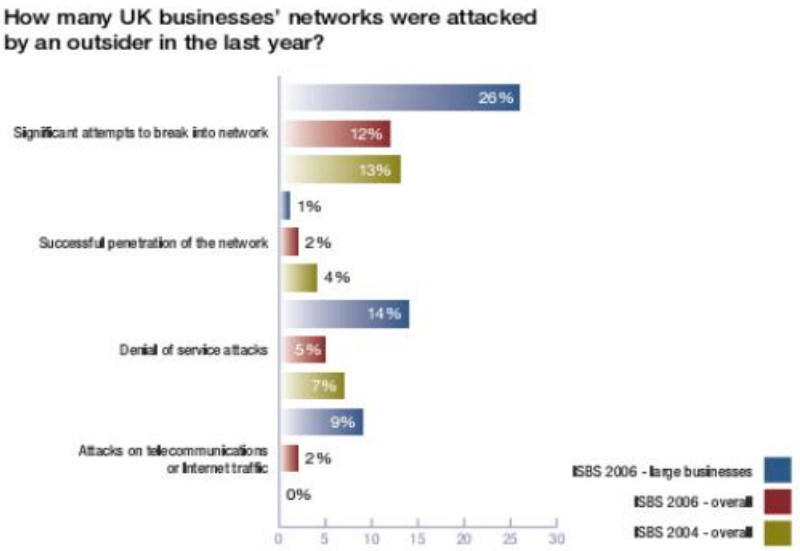
Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.

Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara/terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:



Gambar 2.2 Grafik persentase ancaman keamanan sistem informasi

Survey tersebut juga menunjukkan bahwa 60% organisasi mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan. Kegagalan sistem keamanan lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Faktor internal ini diantaranya kesalahan dalam pengoperasian sistem (40%) dan diskontinuitas power supply (32%). Hasil survey ISBS tahun 2004-2006 menunjukkan bahwa terdapat banyak jaringan bisnis di Inggris (UK) telah mendapatkan serangan dari luar.



Gambar 2.3 UK business network attack

Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

III. Kesimpulan

Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun, bukan hanya sebagai pelengkap sebuah sistem informasi. Dengan adanya pengelolaan keamanan sistem informasi yang baik, maka diharapkan perusahaan dapat memprediksi resiko-resiko yang muncul akibat penggunaan sistem informasi sehingga dapat menghindari atau mengurangi resiko yang mungkin dapat merugikan perusahaan.

Seri ISO/IEC 27000 dapat digunakan sebagai standar untuk pengelolaan keamanan sistem informasi. Penggunaan seri ISO/IEC 27000 dapat disesuaikan dengan kebutuhan yang diperlukan perusahaan untuk mencapai sasaran perusahaan terhadap keamanan sistem informasi. ISO/IEC 27001 memberikan gambaran umum mengenai kebutuhan yang dibutuhkan perusahaan/organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Dalam hal ini untuk memenuhi standar ISMS perusahaan perlu mengetahui gambaran umum kebutuhan dan cakupan dari ISMS yang tertuang dalam ISO/IEC 27001.

IV. Daftar Pustaka

[1] Chazar Chalifa, (2015): *Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005*

[2] M. Bakri, Nia Irmayana: *Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001.* Bandar Lampung

[3] Hendy Maulana Jaya Saputra, dkk: *Kebijakan-Kebijakan Iso 17799 Pada Organisasi Sebagai Manajemen Sistem Keamanan Informasi.* Institut Teknologi Kalimantan

[4] Budi Triandi: *Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0.* Medan

[5] Titus Kristanto, dkk: *Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ.* Surabaya.

BrightTALK

Certificate of Attendance

This is to certify that:

Ilham Eka Putra

Mahasiswa, Universitas Sriwijaya

Viewed:

Securing Your Remote Workforce with Forescout

On: April 26, 2020
For: 1 of 34 minutes

Presented by:

Eduard Serkowitsch, Principal Systems Engineer & Jan Hof, EMEA Marketing Director, Forescout Technologies

April 26, 2020
Date

www.brighttalk.com/webcast/13811/399281
Content link