ANALISIS MANAJEMEN KEAMANAN JARINGAN DENGAN MENERAPKAN STANDAR ISO

Fitriani

Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Abstrak

Manajemen keamanan informasi dilakukan agar informasi tersebut tetap terjaga integritas, kerahasiaan, dan ketersediaannya sehingga dapat meminimalisirkan kerugian apabila terjadi hal-hal yang tidak diinginkan. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Apabila mengganggu performa sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Keamanan selalu saja menjadi isu menarik dalam perkembangan komunikasi, interaksi, dan sosialisasi manusia bahkan di dunia pendidikan. ISO 27001 merupakan suatu standar internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan Information Security Management Systems (ISMS). Menerapkan standar ISO 27001 akan membantu organisasi dalam membangun dan memelihara sistem manajemen keamanan informasi. Sistem manajemen keamanan informasi merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan.

I. Pendahuluan

Pernahkah anda berpikir jika manajemen keamanan informasi saat ini sangat diperlukan. Bagaimana jika tidak adanya manajemen keamanan informasi. Standar yang digunakan dalam penelitian adalah standar ISO 27001:2005 . Dikarenakan standar ISO 27001:2005 merupakan standar yang mudah digunakan sesuai dengan kebutuhan organisasi, tujuan organisasi, proses bisnis, dan jumlah pegawai dari struktur organisasi pendidikan. Pada standar ISO 27001:2005 menyediakan berbagai rekomendasi manajemen keamanan informasi dan layanan IT, serta menyediakan sertifikasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional[1]. Berdasarkan hasil penelitian yang dilakukan, maka diperoleh beberapa temuan antara lain: keamanan laboratorium FTI-UKSW belum memiliki Standard Operational Procedures (SOP) secara tertulis tetapi hanya disampaikan secara lisan sehingga kebijakan-kebijakan yang adapun juga disampaikan secara lisan. Pihak ketiga yang ada di FTI-UKSW juga hanya mengkontrol sistemsistem yang ada tetapi tidak mengambil bukti untuk dokumentasikan. Kontrol akses setiap pengguna tidak di dokumentasikan secara tertulis tetapi diakses pada sistem audit keamanan FTI sendiri. Manajemen pencegahan akses dari luar untuk masuk ke sistem informasi tidak diatur secara tertulis tetapi hanya disampaikan secara lisan dan setiap mengontrol sistem tidak didokumentasikan. Prosedur-prosedur dalam keamanan hanya menyampaikan adanya perubahan sistem dan tidak didokumentasikan kepada karyawan[2].

II. Tinjauan Pustaka

a. Penelitian Terkait

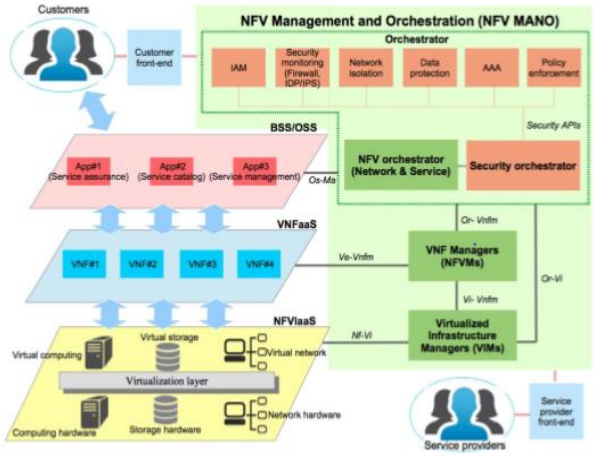
Informasi adalah sumber daya berharga yang sangat penting untuk keberhasilan organisasi, tetapi juga rentan terhadapnya berbagai serangan baik dari dalam maupun dari luar organisasi[3]. Manajemen keamanan informasi dilakukan agar informasi tersebut tetap terjaga integritas, kerahasiaan, dan ketersediaannya sehingga dapat meminimalisirkan kerugian apabila terjadi hal-hal yang tidak diinginkan. Keamanan informasi tegantung pada proses, teknologi, dan orang[4]. Tujuan MKI adalah untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dan untuk mengurangi berbagai risiko dan ancaman terhadap informasi tersebut. Padahal informasi keamanan telah secara konsisten diidentifikasi di bagian atas agenda Sistem Informasi. Manajemen Keamanan

Informasi adalah cara sumber daya ini dikonfigurasikan untuk memenuhi tujuan Keamanan Informasi yang, pada gilirannya, berkontribusi pada keberhasilan organisasi. Manajemen Keamanan Informasi yang baik melegitimasi fungsi dalam konteks organisasi yang lebih luas dan memberikan bukti pendekatan yang matang kepada pihak ketiga. Akhirnya, membantu membangun Keamanan Informasi sebagai sebuah profesi[5]. Bagi organisasi informasi adalah sebuah asset, jika informasi memiliki nilai, integritas dan yang lain nya. Informasi yang dimaksud dapat berupa informasi yang berada pada selembar kertas, tersimpan dalam database, yang dikirimkan melalui surat biasa atau e-mail, video, atau catatan pembicaraan rapat organisasi. Semua informasi tersebut memiliki nilai yang unik bagi setiap organisasi yang mana jika terjadi kebocoran atau kehilangan maka organisasi tersebut dapat mengalami kerugian yang bersifat nyata (tangible) ataupun tidak nyata (intangible).

Dalam penelitian ini, metodologi baru untuk manajemen keamanan optimal infrastruktur kritis telah diuraikan. Model yang diusulkan merupakan kerangka kerja yang fleksibel berdasarkan diagram pengaruh memori terbatas (LIMID) untuk memasukkan berbagai variabel dan berbagai informasi untuk mengembangkan strategi yang efektif terhadap serangan yang disengaja[6]. LIMID yang dikembangkan dapat digunakan untuk memperoleh

(i) Informasi tentang preferensi musuh yang diberikan sistem keamanan,
(ii) Informasi tentang musuh yang diberi skenario,
(iii) Strategi optimal,
(iv) Respons optimal untuk menghadapi serangan.

Data input yang diperlukan untuk memenuhi probabilitas bersyarat (diberikan serangan segera) dari model terutama dinilai oleh para ahli sesuai dengan pengalaman mereka, memaparkan metodologi untuk tingkat subjektivitas. Salah satu kontribusi utama kami mengenai bagian ini adalah untuk menyelidiki kelayakan dan keefektifan manajemen keamanan dan orkestrasi, bagaimana hal itu dapat diotomatisasi dan diatur secara mulus di berbagai platform cloud, dan bagaimana hal itu dapat secara cerdas menegakkan fungsi keamanan untuk melayani permintaan multi-sewa. Seperti yang kami yakini meskipun sebagian besar fungsi keamanan dalam skenario aplikasi tipikal dapat diterapkan ke NFV[7]. Dengan demikian, kami bermaksud untuk mengusulkan desain konseptual manajemen keamanan dan orkestrasi NFV[7].



Gambar 1. Desain konseptual SecMANO yang dapat berupa built-in atau addon dari platform orkestrasi yang ada[7]

b. Tinjauan Pustaka

Keamanan informasi berkaitan dengan melindungi asset informasi terhadap kehilangan atau kerusakan data untuk menjamin kelangsungan bisnis (business continuity) dan meminimalkan resiko bisnis (reduce business risk). Keamanan informasi bisa dicapai dengan beberapa strategi yang bisa dilakukan berupa kombinasi satu dengan yang lain dan mempunyai focus masing-masing dalam strategi sesuai dengan kebutuhan[2]. Pemeriksaan kompleks terhadap masalah keamanan menyiratkan tidak hanya kualitas dasar tetapi juga masuk akal prosedur yang mencapai tujuan karya ilmiah, yaitu metodologi. Melakukan hal itu membutuhkan lebih dari sekadar pendekatan dan metode tradisional. Artikel ini adalah arefleksi pada dimensi baru spesialisasi "Ahli sektor infrastruktur kritis" yang diidentifikasi dalam konteks Sains dan Teknologi dari Slovakia Republik. Nyakonten berfokus pada spesifik pendekatan metodologis untuk mengatasi masalah sektor keamanan, konsep keamanan manusia, tetapi terutama untuk mengeksploitasi alat teoritis potensial yang baru teori yang dihasilkan dari manajemen risiko keamanan[8].

Standar ISO 27001:2005 merupakan standar keamanan informasi berupa persyaratan yang harus dilakukan dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ISO 27001:2005 bersifat independen terhadap produk dari teknologi informasi dan dirancang untuk melindungi asset informasi dari berbagai ancaman atau resiko dari pihak yang tidak bertanggung jawab. ISO 27001:2005 mendefinisikan 133 kontrol keamanan yang terstruktur dan membagi menjadi 11 klausul control keamanan, 39 obyektif control dan 133 kontrol keamanan. Pengelompokkan control keamanan sangat diperlukan untuk memudahkan organisasi instansi pendidikan dalam mengontrol keamanan yang dibutuhkan baik secara manajemen, operasional, maupun teknikal[1].

III. Metode Penelitian

Metode penelitian yang digunakan dalam melaksanakan audit keamanan informasi.

A. Pengumpulan Data Ada beberapa teknik atau cara pengumpulan data yang digunakan dalam penelitian yaitu :

a. Wawancara Tim peneliti melakukan wawancara secara langsung dengan Staff IT Support instansi pendidikan.

b. Studi Lapangan Tim peneliti melakukan studi lapangan berupa pengamatan dan kunjungan langsung ke instansi pendidikan.

c. Studi Literatur Studi literature yang dilakukan tim peneliti berupa pencarian literature atau referensi dari buku, jurnal, dan prosiding yang terkait dengan ISO 27001:2005.

B. Identifikasi Proses Bisnis dan IT

Pada perencanaan audit keamanan informasi, tim peneliti harus memahami proses bisnis dan IT yang ada di instansi pendidikan. Pemahaman yang harus dipelajari oleh tim peneliti adalah mempelajari dokumen yang berhubungan dengan data instansi pendidikan yaitu profil instansi, visi dan misi instansi, struktur organisasi instansi, serta proses dan bisnis IT instansi pendidikan. Tim peneliti harus mengetahui apakah instansi pendidikan tersebut sudah melakukan proses audit atau belum.

C. Menentukan Ruang Lingkup dan Tujuan Audit Sistem Informasi

Pada ruang lingkup yang dilakukan dalam penelitian dengan melakukan wawancara dengan Staff IT Support, studi lapangan, dan studi literature. Hasil dari wawancara dengan Staff IT Support adalah terdapat kekurangan dan kelemahan pada keamanan asset, informasi, dan akses dari aplikasi. Penerapan hasil dari ruang lingkup menggunakan standard ISO 27001:2005, termasuk klausul-klausul yang digunakan pada standard ISO 27001:2005. Pada Tabel 1 merupakan pemetaan dari klausul ISO 27001:2005 berdasarkan hasil wawancara dengan Staff IT Support.

D. Melaksanakan Audit Kepatutan

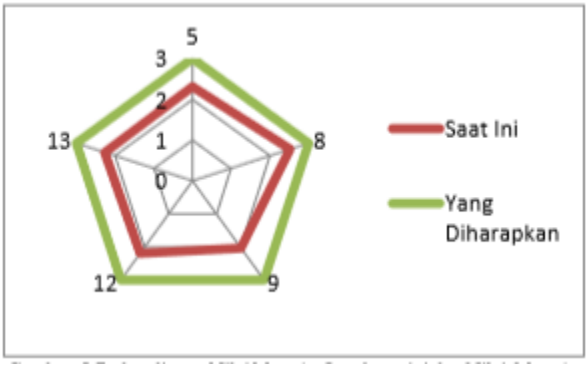
Pada pelaksanaan audit kepatutan menghasilkan dokumen wawancara dengan Staff IT Support, bukti audit, temuan audit, dan tingkat nilai kematangan dari control keamanan. Dari semua bukti yang ada, tahap selanjutnya melakukan analisis dan evaluasi hasil nilai tingkat kemampuan dari tiap control keamanan informasi.

E. Menentukan Maturity Level

Dari hasil penentuan nilai yang ditetapkan, tahap berikutnya adalah membuat Maturity Level. Pada pengelolaan dan pengendalian maturity level berdasarkan pada metode evaluasi organisasi sehingga dapat dievaluasi dari level 0 (tidak ada) hingga level 5 (optimistis).

IV. Pembahasan

Standar ISO 27001:2005 yang digunakan adalah bagian Kontrol Keamanan (Security Control) yang terdiri dari 39 obyektif control dan 133 kontrol keamanan. Untuk mengetahui control-kontrol yang lemah, maka manajemen instansi pendidikan mengambil tindakan untuk memperbaiki control-kontrol yang butuh penanganan. Nilai maturity level didapatkan dari hasil rata-rata jawaban responden yang terdapat pada klausul ISO 27001:2005. Berdasarkan hasil dari maturity level penyebaran kuesioner kepada responden, kemudian dihitung nilai kesenjangan antara maturity level saat ini dengan maturity level yang diinginkan.



Gambar 2. Perbandingan Nilai Maturity Level saat ini dan Nilai Maturity Level yang diharapkan

Berdasarkan hasil perhitungan maturity level keamanan informasi, tingkat keamanan informasi yang sebagai pedoman berada di Level 3 (Defined Process). Berdasarkan hasil perhitungan maturity level yang sudah dilakukan, maka tingkat kematangan keamanan informasi pada bagian IT Support instansi pendidikan rata-rata berada di Level 2 (Managed Process). Berarti keamanan informasi pada instansi pendidikan perlu adanya perbaikan dan perlu

dikembangkan pada tahap selanjutnya yang lebih baik, dikarenakan masih berada di Level 2 (Managed Process).

V. Kesimpulan

Berdasarkan hasil penelitian dapat disimpulkan yaitu :

1. Tingkat kematangan maturity level keamanan informasi pada bagian IT Support instansi pendidikan rata-rata berada di Level 2 (Managed Process) untuk klausul Kebijakan Keamanan Informasi; Keamanan Fisik dan Lingkungan; Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi; Manajemen Penanganan Insiden Keamanan Informasi. Sedangkan klausul Keamanan Sumber Daya Manusia berada di Level 3 (Defined Process).

2. Penerapan dari standarisasi keamanan informasi pada bagian IT Support instansi pedidikan berdasarkan kebutuhan operasional dan teknikal.

3. Responden berasal dari bagian Staff IT Support instansi pendidikan.

DAFTAR PUSTAKA

[1] T. Kristanto, M. Sholik, D. Rahmawati, and M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001 : 2005 Pada Staff IT Support Di Instansi XYZ," vol. 02, no. 02, pp. 1–4, 2019.

[2] Y. Darmawan and F. A. Wijaya, "Analisis Sistem Manajemen Keamanan Informasi Pada Perguruan Tinggi Menggunakan Iso 27001 : 2013," *Semin. Nas. Sist. Inf. Indones.*, no. November, pp. 6–7, 2017.

[3] C. Z. Tu, *Information & Computer Security Article information : Strategic Value Alignment for Information Security Management : A Critical Success Factor Analysis Bios Dr . Cindy Zhiling Tu is an Assistant professor of Information Systems in the School of Computer*. 2017.

[4] Z. A. Soomro, M. H. Shah, and J. Ahmed, "International Journal of Information Management Information security management needs more holistic approach : A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, 2016.

[5] D. Ashenden, "Information Security management : A human challenge ?," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 195–201, 2008.

[6] A. Misuri, N. Khakzad, G. Reniers, and V. Cozzani, "A Bayesian network methodology for optimal security management of critical infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 191, 2019.

[7] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards network functions virtualization (NFV) based security MANagement and orchestration," *Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Process. with Appl. IEEE Trust. 2016*, pp. 598–605, 2016.

[8] M. Kelemen and J. Jevcak, "Security Management Education and Training of Critical Infrastructure Sectors' Experts," *NTAD 2018 - 13th Int. Sci. Conf. - New Trends Aviat. Dev. Proc.*, pp. 72–75, 2018.