NAMA : MITASARI

NIM : 09011381722122

Integrated Safety & Information Security Management System

ABSTRAK

Information Security Management System (ISMS) adalah pendekatan sistematis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi organisasi. Tujuan artikel ini adalah untuk meningkatkan konsep konvensional keselamatan dan keamanan perusahaan manajemen dengan menggabungkan dua fitur yang saling terkait ini dalam satu konsepsi filosofis dan manajerial. Perlindungan keseluruhan perusahaan, tempat aset data penting disimpan, diproses dan dikirimkan tidak mungkin tanpa menyatukan keamanan dan sifat sistem keamanan. Model terintegrasi arsitektur keselamatan fungsional dan sistem manajemen keamanan yang memenuhi persyaratan standar internasional ditampilkan. Ini mencakup prinsip-prinsip kontrol hukum dan kontrol cybernetic.

Keywords : Safety, Manajemen keamanan TI, Information Security

I. Pendahuluan

Memastikan keamanan yang kompleks (keamanan dan keselamatan). Penggunaan keselamatan dan keamanan sebagai kompleks dan definisi umum diperlukan karena ada beberapa atribut dalam keselamatan dan keamanan seperti keamanan fisik,keamanan informasi dan komputer serta keselamatan fungsional. Keamanan adalah atribut teratas keselamatan dan keamanan untuk sistem yang dipertimbangkan. Informasi teknologi dan sistem, di satu sisi, alat untuk menyediakan keselamatan dan keamanan perusahaan penting dan objek industri / sistem, di sisi lain, sumber kerentanan potensial dan anomali. Kegagalan ini disebabkan karena perangkat lunak / desain dan kesalahan perangkat keras / fisik dan serangan, intrusi gunakan pada kerentanan komponen IT. Komponen ini dapat didefinisikan sebagai IT- keselamatan dan keamanan.

Keamanan informasi merupakan elemen integral dari tugas fidusia. Tujuan dari keamanan informasi adalah untuk melindungi sumber daya organisasi yang berharga, seperti informasi. Dalam standar dan kerangka kerja yang relevan serta dalam literatur ilmiah, ketergantungan yang terus meningkat dari hampir semua organisasi pada pemrosesan informasi yang aman dinyatakan secara praktis adalah pada tahun-tahun terakhir.

Dalam SDN, manajemen keamanan berbasis kebijakan bertujuan untuk menemukan yang lebih cerdas cara untuk membangun kembali kontrol berbutir halus atas jaringan dan perilaku pengguna. Server kebijakan, pada dasarnya, mesin aturan tujuan umum (ekspresi) di mana aturan pada prinsipnya dapat ditulis untuk mencapai hasil yang diinginkan. Hasil ini dapat mencakup tidak hanya manajemen lalu lintas umum, tetapi juga manajemen keamanan berorientasi aliran, pemeliharaan Kualitas Layanan (QoS), inspeksi paket yang mendalam, mekanisme antrian, penyeimbang beban, dll.

II. Method

Model Manajemen Keamanan Informasi mewakili integrasi konsep mencakup beberapa aspek keamanan informasi. Ini menarik dari berbagai bidang, termasuk perangkat lunak kerentanan, penilaian risiko, motivasi serangan, deteksi ancaman, pencegahan, dan biaya keamanan. Ini berdasarkan pada model sebelumnya untuk manajemen keamanan informasi.

Model telah ditingkatkan dengan dimasukkannya konstruksi tambahan, dan disempurnakan melalui kalibrasi ulang persamaan untuk memastikan itu situasi yang berpotensi anomali dicegah.

Kriteria dasar berikut untuk proses inti ISMS diidentifikasi dan dikonfirmasi dalam penelitian sebelumnya oleh penulis:
Kriteria 1 - Keteraturan - tugas yang saling terkait dan berinteraksi diulangi secara teratur;
Kriteria 2 - Transformasi - input ditransformasikan menjadi output;
Kriteria 3 - Secara operasional - proses dilakukan saat mengoperasikan ISMS;
Kriteria 4 - Akuntabilitas / tanggung jawab - petugas keamanan informasi adalah pemilik proses atau manajer proses dan proses adalah kompetensi inti dari ISMS;
Kriteria 5 - Menghasilkan nilai - memberikan nilai yang jelas dan langsung kepada pemangku kepentingan.

Untuk identifikasi proses, metode berikut digunakan:

1. Awalnya seri ISO 27000 dianalisis tentang proses yang disebutkan.
2. ITIL dan COBIT dianalisis (cocok) tentang proses ISMS yang sudah diidentifikasi dalam seri ISO 27000 serta tentang kemungkinan proses ISMS tambahan. Tabel yang cocok tentang kemungkinan proses ISMS dibuat untuk ITIL dan COBIT.
3. Hasil dari langkah satu dan dua diringkas dalam tabel pemetaan yang didokumentasikan dalam Haufe.

III. Hasil Analisis

3.1 Keamanan dan Manajemen Informasi

Peran manajemen dalam manajemen keamanan informasi. Dalam aspek yang lebih luas, manajemen memiliki tanggung jawab inti urusan bisnis, sehingga memiliki dampak signifikan pada masing-masing kegiatan bisnis. Keamanan informasi terutama merupakan manajemen dan masalah bisnis, sehingga manajer puncak harus menyadari pentingnya pengembangan dan implementasi kebijakan keamanan informasi dan harus lebih memperhatikan untuk secara efektif melakukan pra-setel kontrol keamanan. Faktor organisasi seperti jenis industri, ukuran organisasi dan struktur sangat mempengaruhi implementasi manajemen keamanan informasi. Organisasi keuangan besar relatif lebih sensitif terhadap efektivitas manajemen keamanan informasi karena potensi ancaman keamanan yang lebih tinggi. Selain dari pengembangan informasi kebijakan keamanan, dukungan manajemen juga penting untuk efektif implementasi kebijakan. Struktur organisasi juga sangat penting dalam manajemen keamanan informasi. Manajemen keamanan informasi memerlukan suatu struktur organisasi yang memfasilitasi pelaporan, komunikasi yang efisien, wewenang yang jelas dan alur kerja yang cepat. Pengembangan sistem keamanan informasi tidak cukup untuk mencegah intervensi informasi dari penipu. Yang efektif program dan kebijakan tata kelola keamanan informasi; kualitas dukungan manajemen eksekutif dan ulasan berkelanjutan dan penggabungan perubahan tertentu untuk dipenuhi tantangan baru adalah faktor kunci efektivitasnya. Semua kegiatan ini membutuhkan minat dan perhatian manajemen tingkat yang lebih tinggi, sehingga manajemen puncak peran mungkin penting untuk manajemen keamanan informasi yang efektif. Manajemen bertanggung jawab untuk mengatasi hambatan-hambatan ini dan utama peran harus dimainkan oleh manajemen tingkat atas. Oleh karena itu, manajer keamanan informasi harus mengadopsi pendekatan yang lebih holistic untuk keamanan informasi yang harus mencakup keterlibatan manajemen puncak e-tailor. Teknologi tidak dapat memberikan solusi yang dapat diandalkan untuk kebutuhan dan tantangan keamanan informasi organisasi. Jadi untuk mengatasi masalah informasi yang selalu menantang keamanan, pendekatan yang seimbang dari faktor teknis, manusia dan organisasi akan lebih efektif. Faktor teknis mengenai perencanaan dan akuisisi teknologi baru, alokasi anggaran, dan pembelian perangkat keras dan perangkat lunak adalah kebijaksanaan manajemen. Faktor manusia, misalnya, perburuan bakat, perekrutan personel khusus,

pelatihan karyawan dan motivasi serta pelaksanaan berbagai kebijakan, adalah tanggung jawab manajemen di bawah paying departemen manajemen sumber daya manusia. Faktor organisasi, seperti pengembangan kebijakan keamanan, kesadaran, kepatuhan dan implementasi dari praktik terbaik, adalah pengukuran dasar untuk keamanan informasi. Semua kegiatan ini adalah tanggung jawab manajemen perusahaan, sehingga dapat dikatakan bahwa pendekatan yang lebih holistik harus diadopsi untuk keamanan informasi pengelolaan. Praktek manajerial mengenai teknologi informasi adalah pendorong efektivitas TI. Manajemen memiliki berbagai praktik mengenai teknologi informasi. Praktek investasi yang lebih tinggi telah terbukti untuk lebih banyak perlindungan dan ketahanan terhadap serangan dari penipu dan kendala anggaran telah direalisasikan sebagai hambatan bagi manajemen keamanan informasi. Jadi bisa disarankan agar tidak hanya mengendalikan praktik, tetapi semua praktik manajerial yang lebih baik terkait dengan keamanan informasi akan membuatnya lebih efisien dan selaras dengan bisnis tujuan. Oleh karena itu, manajer keamanan informasi harus mengadopsi pendekatan yang lebih holistik untuk memasukkan praktik manajerial yang lebih baik untuk manajemen keamanan informasi yang efektif.

3.2 Keamanan Informasi dan Integrasi Manajerial Teknis

Integrasi teknis dan kegiatan manajerial untuk manajemen keamanan informasi yang efektif. Karena sistem informasi meliputi perangkat keras dan perangkat lunak, keahlian teknis dalam sistem informasi sama pentingnya dengan profesionalisme manajerial. Keamanan informasi manajemen dapat dibagi menjadi dua bagian utama, yaitu teknis dan manajerial, jadi integrasi kedua aspek ini akan memastikan efektivitas keamanan informasi. Manajemen harus berurusan dengan aspek-aspek non-teknis keamanan informasi seperti pengembangan kebijakan keamanan, kesadaran pelatihan, akuisisi perangkat keras dan lunak keamanan, kontrol internal dan keputusan mengenai pemrosesan data. Tanpa dukungan teknis dari profesional TI dan keamanan, manajemen akan melakukannya merasa kesulitan untuk mengelola keamanan informasi. Di samping itu, profesional TI tidak dapat melindungi sumber daya informasi tanpa dukungan manajemen dan Keterlibatan. Karena itu, dapat disimpulkan bahwa pengamanan aset informasi dan keamanan data dapat dipastikan melalui integrasi teknis dan manajerial kegiatan.

IV. Kesimpulan

Information Security Management System (ISMS) adalah pendekatan sistematis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi organisasi.

Keamanan informasi merupakan elemen integral dari tugas fidusia. Tujuan dari keamanan informasi adalah untuk melindungi sumber daya organisasi yang berharga, seperti informasi. Dalam standar dan kerangka kerja yang relevan serta dalam literatur ilmiah, ketergantungan yang terus meningkat dari hampir semua organisasi pada pemrosesan informasi yang aman dinyatakan secara praktis adalah pada tahun-tahun terakhir. Model Manajemen Keamanan Informasi mewakili integrasi konsep mencakup beberapa aspek keamanan informasi. Ini menarik dari berbagai bidang, termasuk perangkat lunak kerentanan, penilaian risiko, motivasi serangan, deteksi ancaman, pencegahan, dan biaya keamanan.

Keamanan informasi terutama merupakan manajemen dan masalah bisnis, sehingga manajer puncak harus menyadari pentingnya pengembangan dan implementasi kebijakan keamanan informasi dan harus lebih memperhatikan untuk secara efektif melakukan pra-setel kontrol keamanan. Faktor organisasi seperti jenis industri, ukuran organisasi dan struktur sangat mempengaruhi implementasi manajemen keamanan informasi. Organisasi keuangan besar relatif lebih sensitif terhadap efektivitas manajemen keamanan informasi karena potensi ancaman keamanan yang lebih tinggi. Selain dari pengembangan informasi kebijakan keamanan, dukungan manajemen juga penting untuk efektif implementasi kebijakan. Struktur organisasi juga sangat penting dalam manajemen keamanan informasi. Manajemen keamanan

informasi memerlukan suatu struktur organisasi yang memfasilitasi pelaporan, komunikasi yang efisien, wewenang yang jelas dan alur kerja yang cepat. Pengembangan sistem keamanan informasi tidak cukup untuk mencegah intervensi informasi dari penipu.

REFERENCES

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2015.03.054

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27–47. https://doi.org/10.12821/ijispm040402

Kharchenko, V., Dotsenko, S., Illiashenko, O., & Kamenskyi, S. (2019). Integrated Cyber Safety Security Management System: Industry 4.0 Issue. *Conference Proceedings of 2019 10th International Conference on Dependable Systems, Services and Technologies, DESSERT 2019*, 197–201. https://doi.org/10.1109/DESSERT.2019.8770010

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2015.02.002

McLaughlin, D., & Kinzelbach, W. (2015). Food security and sustainable resource management. *Water Resources Research*. https://doi.org/10.1002/2015WR017053

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information and Management*, *52*(1), 123–134. https://doi.org/10.1016/j.im.2014.10.009

Sonntag, M. (2016). Cyber security. *IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks*. https://doi.org/10.2478/hjbpa-2019-0020

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009