Fungsi Manajemen Insiden Keamanan Informasi pada Portal Internal Perusahaan untuk Mendukung Kepedulian Keamanan Informasi

Andy Primawan
23215123 – andyprimawan@gmail.com

Abstrak:

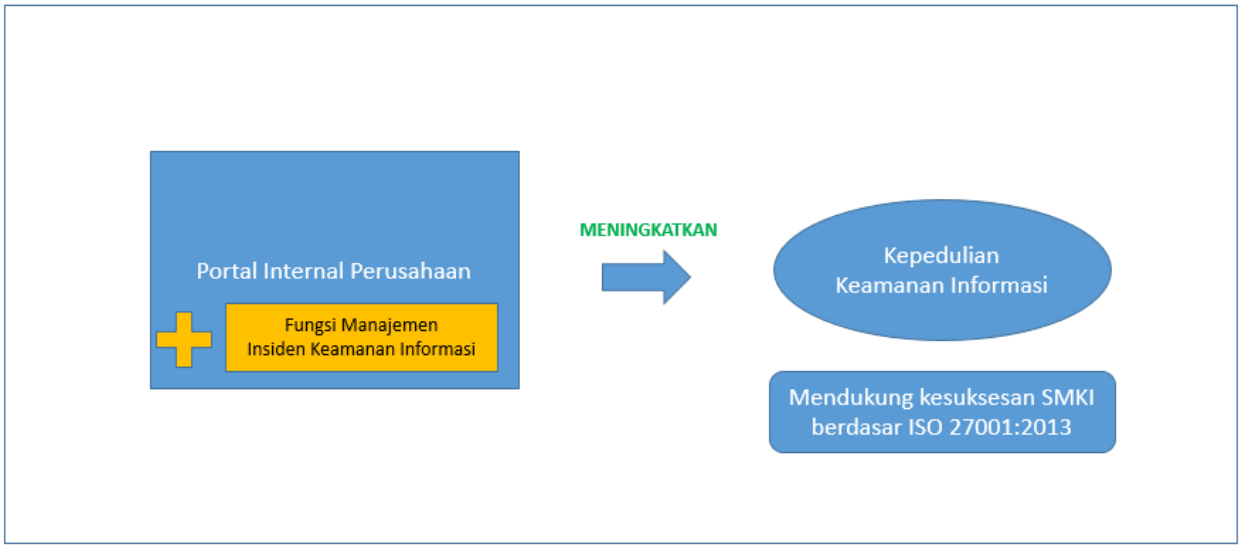
Kepedulian keamanan informasi adalah salah satu faktor yang menentukan kesuksesan implementasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO 27001:2013 di sebuah organisasi. Ada pun kepedulian ada sebagai persyaratan yang wajib dipenuhi berdasarkan standar ISO 27001:2013 bagian 7.3 yang menyatakan seluruh karyawan harus memiliki perhatian yang besar terhadap:

1. kebijakan keamanan informasi;
2. kontribusinya terhadap efektivitas SMKI dan manfaat dari peningkatan kinerja keamanan informasi;
3. akibat dari ketidakpatuhan terhadap persyaratan SMKI.

Di sisi lain sebuah organisasi yang ingin mengimplementasikan Sistem Manajemen Keamanan Informasi berdasarkan standar ISO 27001:2013 dianjurkan untuk merujuk daftar kendali keamanan informasi yang ada di Annex A pada dokumen ISO 27001:2013. Salah satu kendalinya adalah mengenai manajemen insiden keamanan informasi pada poin A16 dengan detil:

1. terdapat tanggung jawab dan prosedur manajemen insiden keamanan informasi,
2. melaporkan kejadian keamanan informasi,
3. pelaporan kelemahan keamanan informasi,
4. penilaian dan keputusan pada kejadian keamanan informasi,
5. menanggapi insiden keamanan informasi,
6. belajar dari insiden keamanan informasi, dan
7. pengumpulan bukti.

Organisasi yang ingin mengimplementasikan SMKI berdasarkan ISO 27001:2013 tentu saja akan menemui rintangan. Organisasi perlu menumbuhkan kepedulian keamanan informasi kepada seluruh karyawan yang terlibat yang tentu saja tidak seluruhnya memiliki latar belakang teknologi informasi. Saya melihat portal internal perusahaan dapat dimanfaatkan sebagai sarana dan alat untuk penyampaian pesan untuk meningkatkan kepedulian terhadap keamanan informasi.



Di sisi lain saya juga melihat insiden keamanan informasi yang terjadi dapat menjadi bukti kasus agar karyawan menjadi lebih peduli terhadap keamanan informasi. Sehingga inti dari penelitian pada kelas ini fokus pada manajemen penanganan insiden keamanan informasi dengan inti:

1. memanfaatkan portal internal perusahaan untuk meningkatkan kepedulian keamanan informasi,
2. menambahkan fitur manajemen insiden keamanan informasi pada portal internal perusahaan, dan
3. memanfaatkan insiden keamanan informasi yang direkam di portal internal perusahaan sebagai contoh insiden keamanan informasi, untuk meningkatkan kepedulian keamanan informasi.

Referensi

Paper Penelitian yang berkaitan dengan topik penelitian ini dari koleksi **IEEE Explore** dan **Springer Link** (urutan tidak menunjukkan tingkat keterkaitan) antara lain:

1. Prerequisites for building a Computer Security Incident Response capability. 2015
2. Approaches to improve the activity of computer incident response teams. 2015
3. The Future of Incident Response. 2014
4. IRSS: Incident Response Support System. 2006
5. A Security Coordination Model for an Inter-Organizational Information Incidents Response Supporting Forensic Process. 2008
6. Computer Security Incident Response Team Development and Evolution. 2014
7. An incident response support system based on seriousness of infection. 2016
8. A GRReat framework for incident response in healthcare. 2015
9. Collaboration Engineering for Incident Response Planning: Process Development and Validation
10. Cerebro: A Platform for collaborative incident response and investigation. 2013
11. Device Independent Information Sharing During Incident Response. 2008
12. Modeling Fraud Prevention of Online Services Using Incident Response Trees and Value at Risk. 2015
13. Developing a Community Cyber Security Incident Response Capability. 2009

14. Dynamic cyber-incident response. 2014
15. An Industrial Control Systems incident response decision framework. 2015
16. A Security Incident data model. 2002
17. An Investigative Framework for Incident Analysis. 2011
18. Improving the Exchange of Lessons Learned in Security Incident Reports. 2015
19. Information Technology Incident Management. 2012
20. Internalization of Information Security Culture amongst employees through basic security knowledge. 2006
21. Security Modelling for Risk Analysis. 2004
22. Security Transparency: the next frontier for security research in the cloud. 2015