Perancangan dan Analisa Kebijakan Manajemen Insiden Keamanan Informasi pada Pusat TIK Lembaga XYZ menggunakan Standar ISO / IEC 27035 = Design and Analysis of Information Security Incident Management Policy at the ICT Center of XYZ Institution using ISO/IEC 27035 standard

Ismail Yusry, author

Abstrak

Ancaman terhadap keamanan informasi menjadi hal yang sering dijumpai saat ini baik di lingkup individu maupun organisasi. Beberapa jenis ancaman tersebut berasal dari serangan virus, malware, web defacement dan phising. Untuk mengantisipasi dan merespon serangan tersebut, lembaga XYZ membentuk tim insiden respon atau yang dikenal sebagai CSIRT (Computer and Security Incident Response Team). Penanganan insiden keamanan informasi merupakan aspek kritis dalam memastikan integritas dan kelangsungan operasional suatu organisasi. Berdasarkan catatan, insiden keamanan informasi masih sering terjadi hingga saat ini di lingkungan organisasi.

Penelitian ini bertujuan untuk melakukan analisis terhadap pendekatan yang diambil oleh organisasi dalam menangani insiden keamanan informasi dengan area fokus pada efektivitas langkah-langkah yang dilakukan. Kerangka kerja yang digunakan adalah ISO/IEC 27035:2016, terdapat 69 klausul dilakukan untuk mengevaluasi penanganan insiden dan 62 klausul untuk diterapkan untuk perencanaan kebijakan penanganan insiden. Hasil asesmen pada lembaga XYZ menggunakan ISO/IEC 27035 mengenai manajemen insiden keamanan informasi didapatkan bahwa organisasi telah menerapkan sejumlah 53% dari 69 klausul yang diterapkan.
.....Threats to information security are something that is often encountered today, both in individuals and organizations. Several types of threats come from virus attacks, malware, web defacement and phishing. To anticipate and respond to these attacks, XYZ Institution formed an incident response team or known as CSIRT (Computer and Security Incident Response Team). Handling information security incidents is a critical aspect to ensuring the integrity and operational continuity of an organization. Based on records, information security incidents still frequently occur today in organizational environments.

This research aims to conduct an analysis of the approaches taken by organizations in handling information security incidents with a focus area on the effectiveness of the steps taken. The framework used is ISO/IEC 27035:2016, there are 69 clauses to evaluate incident handling and 62 clauses to be applied for planning incident handling policies. The results of an assessment at XYZ institution using ISO/IEC 27035 regarding information security incident management found that the organization had implemented 53% of the 69 clauses implemented.