Analisis Layanan CSIRT Dalam Menghadapi Tantangan Keamanan Siber di Indonesia = Analysis Of CSIRT Services in Facing Cyber Security Challenges in Indonesia

Muhammad Haidar, author

Abstrak

Seiring dengan perkembangan teknologi informasi yang pesat dan mendukung beberapa aspek kehidupan, peningkatan pemanfaatan teknologi informasi tersebut berbanding lurus dengan resiko keamanan. Dalam penanganan keamanan teknologi informasi, terdapat Indeks Keamanan Informasi (KAMI) yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Salah satu faktor yang menentukan nilai indeks KAMI 4.1 ialah tata Kelola keamanan informasi yang memiliki definisi kebijakan dan langkah penanggulangan insiden keamanan informasi CSIRT (Computer Security Incident Response Team) merupakan suatu organisasi atau tim yang bertanggung jawab untuk menerima, meninjau dan menaggapi laporan dan aktivitas insiden keamanan siber. Namun sejak CSIRT berdiri, layanan CSIRT di Indonesia saat ini belum banyak berubah dari pertama dicanangkan, yang berubah hanya teknologi dan beberapa Teknik penyerangan dan pertahanan siber namun prinsip-prinsip manajemennya dinilai tetap sama. Penelitian ini bertujuan untuk melakukan analisis peran dan layanan CSIRT di Indonesia untuk menghadapi ancaman serangan siber dengan menggunakan framework Carnegie Mellon University (CMU). Hasil dari penelitian ini ialah berupa rekomendasi dengan melakukan pemetaan dari hasil penelitian terhadap framework FIRST sehingga didapatkan 10 rekomendasi yang dapat di berikan terhadap implementasi layanan CSIRT di Indonesia.

..... Along with the rapid development of information technology and supporting several aspects of life, the increase in the use of information technology is directly proportional to the risk of cyber security. To handle information technology security, there is an Information Security Index (KAMI) which is used as a tool to assess and evaluate the level of readiness (Completeness and Maturity) of the application of information security based on the criteria of SNI ISO/IEC 27001. One of the factors that determine the value index KAMI 4.1 is Information security governance which has a definition of information security incident response policies and measures CSIRT (Computer Security Incident Response Team) is an organization or team responsible for receiving, reviewing, and responding to cybersecurity incident reports and activities. However, since CSIRT was established, the current CSIRT service in Indonesia has not changed much from when it was first launched, only technology and some cyber attack and defense techniques have changed but the management principles are considered to remain the same. This study aims to analyze the role and services of CSIRT in Indonesia to deal with the threat of cyber attacks using the Carnegie Mellon University (CMU) framework. The results of this study are recommendations by mapping the results of research against the FIRST framework so that 10 recommendations can be obtained for the implementation of CSIRT services in Indonesia.