Penerapan manajemen insiden dalam sistem siber sebagai instrumen intelijen keamanan = The implementation of incident management in cyber systems as a security intelligence instrument

Rizky Hendra Kurniawan, author

Abstrak

Framework manajemen insiden merupakan sebuah tools yang dapat digunakan sebagai early warning system dalam mengatasi permasalahan penerapan teknologi informasi di ranah siber. Framework ini juga dapat menjadi sumber informasi intelijen yang bersifat terbuka dan dapat digunakan untuk mengukur sejauh mana tingkat kematangan manajemen insiden yang telah dilakukan oleh institusi/perusahaan di Indonesia. Dalam lingkup nasional, framework ini juga dapat digunakan untuk melihat sejauhmana kemampuan Indonesia dalam menghadapi terjadinya insiden siber. Hal ini sangat penting mengingat framework manajemen insiden belum diterapkan secara masif oleh institusi/perusahaan di Indonesia, sehingga masih banyak terdapat celah-celah kerawanan yang dapat dimanfaatkan oleh penyerang dalam melakukan cipta kondisi terhadap insiden keamanan siber. Oleh karena itu, penulis melakukan penelitian terkait penerapan framework manajemen insiden ini. Metode penelitian yang digunakan berupa mix-method, dimana merupakan perpaduan dari metode kualitatif dan kuantitatif. Selain itu, teknik analisis data yang digunakan berupa comparative analysis dan content analysis. Hasil dari penelitian ini diantaranya: (1) Nilai koefisien potensi ancaman terhadap pengelolaan intelijen keamanan siber adalah 15.86. Nilai tersebut termasuk dalam kategori tinggi (high); (2) Kerangka kerja (framework) manajemen insiden yang dihasilkan terdiri dari 354 aktifitas manajemen insiden, yang dapat diimplementasikan oleh institusi/perusahaan, dan terbagi dalam 50 kategori pada framework manajemen insiden. Selain itu, distribusi aktifitas dalam framework terdiri dari 12.4% berasal dari SIM3 Model, 42.1% berasal dari Joao Model, dan 70% berasal dari CREST Model.
.....The incident management framework is a tools that can be used as an early warning system to overcome problems in the implementation of information technology. This Framework also used for measuring the maturity level of incident management that has been carried out by institutions in Indonesia. We can used it as an open intelligence of information source. Within national scope, this framework used for knowing Indonesia's ability to deal with cyber incidents. This is very important thing considering that the incident management framework has not been implemented massively by institution in Indonesia. This causes many vulnerabilities than can be exploited by an attacker for creating new conditions in cybersecurity incident. Therefore, author employed mix-methode research, which is the combination between qualitative and quantitative research. The data analysis techniques used were comparative analysis and content analysis. The result of this research are: (1) coefficient value of potential threat to cybersecurity intelligence management is 15.86. This value is included in high category; (2) This research produces a incident management framework that consisting of 354 incident management activity, which are divided into 50 incident management category. Furthermore, the distribution of incident management activity are consist of 12.4% SIM3 Model, 42.1% Joao Model, and 70% CREST Model.