Pengembangan Kerangka Kerja Respon Insiden Keamananan Siber Pada Operational Technology (OT) = Development of a Cybersecurity Incident Response Framework in Operational Technology (OT)

Andri Tri Prasetyo, author

Abstrak

Meningkatnya serangan siber terhadap teknologi operasional (OT) pada infrastruktur kritis mengharuskan setiap pemilik aset atau infrastruktur menyiapkan metode yang sesuai untuk merespons dan menangani insiden keamanan siber. Untuk menghindari risiko dalam pengelolaan insiden keamanan siber di lingkungan OT, diperlukan kerangka kerja yang dapat membantu pemilik infrastruktur menyelesaikan insiden. Penelitian ini berfokus pada pengembangan kerangka respons insiden keamanan siber OT berdasarkan berbagai standar dan praktik terbaik untuk mengelola insiden keamanan siber di sektor OT. Beberapa standar tersebut dipetakan sehingga menghasilkan sejumlah fase utama yang di dalamnya terdapat aktivitas kerangka kerja dan poin-poin rekomendasi implementasi. Hasil penelitian ini berupa kerangka kerja yang terdiri dari 4 fase utama, 12 kegiatan, dan 38 rekomendasi implementasi. Untuk memvalidasi kerangka kerja yang diusulkan, dilakukan metode kuantitatif berdasarkan penilaian ahli (expert) untuk mengukur kepercayaan antar para ahli mengenai rekomendasi implementasi kerangka kerja menggunakan statistik Fleiss Kappa. Pengukuran tersebut menghasilkan nilai kappa sebesar 0,7597 dan dikategorikan kesepakatan substansial yang menunjukkan bahwa beberapa ahli telah menyepakati rekomendasi kerangka kerja.

.....The increase in cyberattacks against operational technology (OT) in critical infrastructure requires every asset or infrastructure owner to prepare suitable methods for responding to and handling cybersecurity incidents. To avoid risks in managing cybersecurity incidents in OT environments, a framework is needed that can help infrastructure owners resolve incidents. This research focuses on developing an OT cybersecurity incident response framework based on various standards and best practices for managing cybersecurity incidents in the OT sector. Some of these standards were mapped to produce a number of key phases in which the framework activities and points of implementation recommendations were included. The result of this research is a framework consisting of 4 main phases, 12 activities and 38 implementation recommendations. To validate the proposed framework, a quantitative method based on expert judgment was conducted to measure the trust between experts regarding the framework implementation recommendations using Fleiss Kappa statistics. The measurement resulted in a kappa value of 0.7597 and was categorized as substantial agreement, indicating that several experts had agreed on the framework recommendations.