Perancangan Kerangka Kerja Network Security Operation Center (NSOC): Studi Kasus Kementerian Luar Negeri = Network Security Operation Center (NSOC) Framework Design: A Case Study of the Ministry of Foreign Affairs

Fitri Wijayanti, author

Abstrak

Hasil penilaian indeks KAMI dari tahun ke tahun menyatakan bahwa sistem elektronik yang dikelola Kementerian Luar Negeri termasuk dalam kategori strategis, sehingga jika mengalami kegagalan akan berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara. Laporan bulanan monitoring Pokja Network Security Operation Center (NSOC) Pustik KP Kemlu menunjukkan bahwa intensitas serangan siber yang ditujukan ke fasilitas TIK Kemlu sangat intensif. Sementara itu fasilitas Data Center Kemlu di Pejambon juga mengalami downtime dengan rata-rata SLA 97,23% pada tahun 2019. Aset yang strategis, tingginya ancaman dan vulnerability layanan, membuat Pustik KP selaku pengelola layanan TIK Kemlu membentuk Pokja NSOC yang bertugas melakukan monitoring terhadap ketersediaan layanan TIK dan keamanan informasi di Kemlu. Namun pada pelaksanaannya pokja NSOC memiliki kesulitan dalam pelaksanaan tugas dan fungsinya disebabkan oleh tidak terdefinisinya kerangka kerja NSOC yang meliputi objektif, batasan, proses bisnis dan aliran data serta dukungan SDM dan teknologi yang optimal. Guna menjawab permasalahan tersebut, penelitian ini disusun dengan menggunakan kerangka kerja NIST Cyber Security Framework. Metodologi penelitian yang digunakan adalah Design Science Research (DSR) dengan metode pengumpulan data melalui observasi, studi dokumen dan wawancara. Hasil dari penelitian ini adalah sebuah rancangan kerangka kerja Network Security Operation Center yang dapat diimplementasikan di Kementerian Luar Negeri.

..... Index KAMI assessment result, from year to year, state that the electronic system of the Ministry of Foreign Affairs are categorize as strategic. That if it fails, it will have a serious impact on the public interest, public service, business process of the state, or national defense and security. The monthly monitoring report of the Pokja Network Security Operations Center (NSOC) of Ministry of Foreign Affairs shows that the intensity of cyber-attacks aimed at the Ministry's ICT facilities is very intensive. Meanwhile, the Ministry of Foreign Affairs Data Center facility in Pejambon also experienced downtime with an average SLA of 97.23% in 2019. Strategic assets, high threat and vulnerability of services, made the Pustik KP as the management of ICT services in the Ministry of Foreign Affairs form the Pokja NSOC in charge of monitoring the availability of ICT services and information security in the Ministry of Foreign Affairs. However, in its implementation the NSOC working group has difficulties in carrying out its tasks and functions due to the undefined NSOC framework which includes objectives, boundaries, business processes and data flow as well as optimal HR and technology support. In order to answer these problems, this research was prepared using NIST Cyber Security Framework. The research methodology used is Design Science Research (DSR) with data collection methods through observation, document studies and interviews. The result of this study is a draft of Network Security Operation Center framework that can be implemented at the Ministry of Foreign Affairs.