Perancangan kapabilitas SOC dalam pengelolaan insiden siber: studi kasus Badan Siber Sandi Negara = Design capability SOC in cyber incident management: a case study in Badan Siber Sandi Negara

Jenny Irna Eva Sari, author

Abstrak

ABSTRAK
Seiring dengan semakin tingginya serangan siber yang masuk ke Indonesia, Pemerintah memberikan perhatian besar mengenai keamanan siber yaitu dengan menerbitkan Perpres 53 Tahun 2017 tentang Pembentukkan Badan Siber dan Sandi Negara BSSN . Perwujudan hal tersebut dilakukan dengan menata Lembaga Sandi Negara menjadi BSSN guna meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional. Salah satu kegiatan yang mendukung keamanan siber adalah penyelenggaraan Security Operation Center SOC . Kegiatan SOC telah menjadi program prioritas nasional yang dicanangkan Lemsaneg dalam Rencana Kerja Pemerintah RKP Tahun 2017. Urgensi untuk mencapai stabilitas keamanan dan ketertiban dalam kegiatan prioritas keamanan siber, menjadi alasan utama perlunya pengamanan informasi dan komunikasi di lingkungan pemerintahan serta lingkup nasional. Dari hasil penilaian kapabilitas minimum SOC, didapat bahwa hasil penilaian kapabilitas SOC pada BSSN belum optimal dan dibutuhkan perangkat tata kelola khusus untuk mengoptimalisasi kapabilitas SOC. Identifikasi masalah memperlihatkan belum adanya rancangan pengembangan SOC secara menyeluruh berdasarkan kapabilitas SOC dalam pengelolaan insiden siber. Penelitian ini menggunakan kerangka kerja NIST Framework for Improving Critical Infrastructure Cybersecurity sebagai kerangka kerja utama. Metodologi penelitian yang digunakan ialah studi kasus dengan pendekatan Soft System Methodology SSM . Pengumpulan data berupa wawancara, studi dokumen, dan observasi. Hasil dari penelitian ini adalah rancangan pengembangan dan aktivitas untuk meningkatkan kapabilitas dalam menyelenggarakan SOC secara optimal serta memenuhi tujuan dalam terjaminnya keamanan informasi. Rancangan tersebut akan divalidasi oleh kepala Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.
<hr>
ABSTRACT
Due to the increasing number of cyber-attacks coming into Indonesia, the Government gives great attention towards cyber security by issuing Presidential Decree 53 of 2017 on the Establishment of Badan Siber dan Sandi Negara BSSN . The Agency is established by arranging Lembaga Sandi Negara into BSSN in order to increase national economic growth and to achieve national security. One of the activities that support cybersecurity is the establishment of Security Operation Center SOC . SOC 39;s activities have become national priority program launched by Lemsaneg in the Government Work Plan of 2017. The urgency to achieve security and order stability in cybersecurity priority activities becomes the main reason for the need of information and communication security within the government and the national scope. Based on the result of SOC minimum capability assessment, it is found that the SOC capability at BSSN is not optimal yet. To optimize the capability, it needs particular governance tool. The problem identification shows that there is no comprehensive SOC development plan based on SOC capability in managing cyber incidents. This research uses the NIST Framework for Improving Critical Infrastructure Cybersecurity as the main

framework. The methodology used in this research is case study with Soft System Methodology SSM approach. Data collection are in the form of interviews, document studies, and observation. The result of this research is the development and activity design to increase the capability in organizing the SOC optimally and to fulfill the purpose in ensuring the information security aspect. The draft will be validated by the head of the National Cyber Security Operations Center in BSSN.