Perancangan Kapabilitas Security Operations Center (SOC): Studi Kasus PT XYZ = Design of Security Operations Center (SOC) Capabilities: Case Study of PT XYZ

Muhammad Firzi Nabil, author

Abstrak

Cybersecurity atau keamanan siber telah menjadi perhatian utama bagi organisasi dan perusahaan-perusahaan di seluruh dunia. Sebagai salah satu institusi perbankan terbesar di Indonesia, PT XYZ sangat memperhatikan aspek tersebut dengan menerapkan kebijakan keamanan dalam hal tata kelola dan operasional dalam inisiatif perusahaan mereka.
Sayangnya, kebijakan tersebut kurang tercermin untuk anak perusahaan dari PT XYZ. Kebijakan, kerangka, dan alur kerja untuk keamanan siber belum terdefinisikan dan terstruktur sehingga mereka akan lebih rentan terkena dampak dan risiko serangan dan kerentanan siber dibandingkan dengan perusahaan induk. Risiko tersebut termasuk availaibility untuk aplikasi, kerugian finansial, kebocoran data internal dan nasabah, dan masalah dan denda dari regulator.
Untuk menghindari risiko tersebut, maka dibuatlah Security Operations Center (SOC) untuk grup perusahaan. SOC tersebut dibuat agar sinergi atau kesiapan untuk keamanan siber beserta manajemen risiko darinya bagi perusahaan anak lebih setara atau melebihi perusahaan induk. Tanggung jawab dan fungsi mereka mencerminkan kebijakan yang ada di perusahaan induk. Beberapa hasil dan manfaat yang diharapkan adalah sebagai inisiatif strategis, meningkatkan kepercayaan stakeholder, meningkatkan visibilitas keamanan, evaluasi dan peningkatan keamanan, pemenuhan regulasi, menutup celah keamanan, dan meningkatkan kesiapan keamanan siber.
Penelitian ini menggunakan Soft System Methodology (SSM) dengan kerangka kerja NIST Framework. Pengumpulan data berbentuk observasi, studi literatur, dan wawancara. Hasil dari penelitian ini adalah rancangan kapabilitas SOC berupa aktivitas yang perlu dijalankan dan dikembangkan serta diprioritaskan. Rancangan tersebut kemudian akan divalidasikan oleh Team Lead Security Strategy & Management selaku pelaksana SOC di perusahaan induk. Diharapkan dari hasil penelitian ini agar penyelenggaraan SOC di grup perusahaan menjadi efektif serta memenuhi tujuan keamanan siber di lingkup grup perusahaan.
.....Cybersecurity has become a major concern for organizations and companies around the world. PT XYZ is also very concerned about this aspect by implementing security policies in terms of governance and operations in their corporate initiatives.
Unfortunately, the policy is less reflected for XYZ Group subsidiaries. The policies, frameworks, and workflows for cybersecurity have not been defined and structured so that they will be more vulnerable to the impact and risk of cyber-attacks and vulnerabilities compared to the parent company. Such risks include availability for applications, financial losses, internal and customer data leaks, and issues and fines from regulators.
To avoid these risks, a Security Operations Center (SOC) for company group was created. The SOC is created so that the synergy or readiness for cybersecurity and its risk management for subsidiaries is equal to or exceeds that of the parent company. Their responsibilities and functions reflect the policies of the parent company. Some of the expected results and benefits are as a strategic initiative, increasing stakeholder trust,

increasing security visibility, evaluating, and improving security, fulfilling regulations, closing security gaps, and increasing cybersecurity readiness.

This research uses Soft System Methodology (SSM) with the NIST Framework. Data collection is in the form of observation, literature study, and interviews. The result of this research is an SOC capability design in the form of activities that need to be carried out and developed and prioritized. The design will then be validated by Team Lead Security Strategy & Management as the SOC implementer at the parent company. It is expected from the results of this research that the implementation of SOC in the group of companies will be effective and meet cybersecurity objectives within the scope of the company group.