Universitas Indonesia Library >> UI - Tesis Membership

Analisis Kesenjangan Kapasitas Pegawai dalam Mengelola Keamanan Jaringan dan Implementasinya terhadap Pencegahan Ancaman Insider Threat pada Organisasi XYZ = Analysis of Employee Capacity Gap in Managing Network Security and Its Implementation towards Insider Threat Prevention in XYZ Organization

Sitorus, Felix Noel, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920565067&lokasi=lokal

---

Abstrak

Keamanan jaringan sangat penting untuk melindungi informasi organisasi di era digital yang berkembang pesat. Ancaman terhadap jaringan tidak hanya berasal dari luar, seperti malware atau peretasan, tetapi juga dari dalam organisasi, dikenal sebagai ancaman internal (insider threat). Ancaman ini dapat menyebabkan kerugian besar, baik akibat tindakan sengaja maupun tidak sengaja dari karyawan atau pihak internal yang memiliki akses ke sistem. Oleh karena itu, kemampuan pegawai dalam mengelola keamanan jaringan menjadi kunci dalam menghadapi ancaman ini. Penanganan ancaman internal harus menjadi prioritas utama organisasi. Penelitian ini bertujuan untuk menganalisis kesenjangan kapasitas pegawai dalam mengelola keamanan jaringan dan dampaknya terhadap pencegahan ancaman insider threat pada organisasi XYZ. Melalui penerapan standar keamanan ISO 27001, khususnya dalam konteks Sistem Manajemen Keamanan Informasi (SMKI) dengan pendekatan PDCA, penelitian ini mengevaluasi bagaimana pengelolaan sumber daya manusia berhubungan dengan pengelolaan aset informasi dan pemeliharaan keamanan jaringan. Hasil penelitian menunjukkan bahwa kesenjangan kapasitas pegawai dalam hal pengetahuan dan keterampilan terkait keamanan jaringan berkontribusi signifikan terhadap kerentanannya terhadap ancaman insider threat. Penelitian ini juga mengungkapkan bagaimana penerapan ISO 27001, yang mengedepankan analisis aset dan siklus PDCA, dapat membantu organisasi dalam memperbaiki tata kelola keamanan informasi dan mencegah insider threat.

.....Network security is crucial for protecting organizational information in the rapidly evolving digital era. Threats to networks do not only originate from external sources, such as malware or hacking, but also from within the organization, known as insider threats. These threats can cause significant damage, whether due to intentional or unintentional actions by employees or internal parties who have access to the system. Therefore, employees' ability to manage network security is key to addressing these threats. Handling insider threats must be a top priority for organizations. This study aims to analyze the gap in employees' capacity to manage network security and its impact on preventing insider threats at organization XYZ. Through the implementation of ISO 27001 security standards, particularly within the context of the Information Security Management System (ISMS) with a PDCA approach, this research evaluates how human resource management relates to the management of information assets and the maintenance of network security. The results of the study show that the gap in employees' knowledge and skills related to network security significantly contributes to their vulnerability to insider threats. The study also reveals how the application of ISO 27001, which emphasizes asset analysis and the PDCA cycle, can help organizations improve information security governance and prevent insider threats.