Perancangan kebijakan keamanan yang efektif dalam mengahdapi ancaman internal studi kasus: President University

Sasongko Budhi W., author

Abstrak

Fasilitas Teknologi Informasi yang ditawarkan oleh Presiden University yaitu fasilitas internet, email, e-book, file server dan laboratorium komputer, yang perlu dilindungi terhadap ancaman internal dan eksternal. Ancaman internal datang dari pengguna dalam jaringan lokal (Local Area Network). Ancaman internal ini cukup tinggi karena mahasiswa yang selalu ingin mencari dan mencoba menerapkan ilmunya dan terkadang diterapkan secara tidak benar. Untuk itu dibutuhkan kebijakan keamanan sistem informasi yang cukup efektif,. Khususnya untuk menghadapi ancaman-ancaman dari dalam (internal). Karena di satu sisi adanya kebutuhan agar jaringan komputer tetap aman, tetapi di lain sisi aset Teknologi Informasi harus dapat dipergunakan oleh mahasiswa, staf dan dosen setiap saat. Diperlukan adanya identifikasi kebijakan keamanan yang sesuai dengan kebutuhan organisasi. Identifikasi ini berdasarkan pada aset dan resiko yang dapat terjadi karena ancaman internal. Standard dirancang sesuai dengan kebijakan keamanan yang merupakan penerapan teknologi yang mampu mengatasi ancaman internal tersebut.
<hr>
Information technology facility that President University offered are internet, email, e-book, file server and computer laboratory that should be protected from internal and external threat. Internal threats are coming from user in Local Area Network. Internal threats are very high because students always searching and try to implement their knowledge and frequently it is implemented in the wrong way. For that reason it needs effective information security policy, especially to handle internal threats. Because in one side the need of safe computer networking but the other side information technology asset should be used by student, staff and lecturer at any time. It needs identification of security policy that relevant to organization needs. This identification based on asset and risk that can be exploited by internal threats. Standard will be designed related to security policies and should be implementation of technology that can handle internal threats.