ABSTRACT

Data security is an important aspect of information technology advancement in this digital age. Despite increasing data security efforts, data leakage remains a significant threat. The use of OSINT is a very useful tool to assist in mitigating of phishing attacks using auditing and policy based methods by conducting Social Engineering activities and experiments using spear phishing techniques on email content. This can be used to identify security gaps that may need to be fixed. By applying these techniques, it can get a clearer picture of the potential weak points in the system used. This research implements experiments using OSINT tools, social engineering activities, and email content. OSINT experiments and phishing attacks are presented in the form of Data Flow Diagrams to show the flow of the attacks carried out. The email content experiments are formulated using Activity Diagrams which are used to visualize mitigation steps using auditing and policy based methods. This method includes the application of continuous auditing and policies such as the UU PDP and the design of appropriate SOP in maintaining data security in the face of phishing attacks. Integrating auditing and policy enables the implementation of a more structured and effective result-oriented mitigation strategy to protect data from potential leaks and strengthen the overall security system.

Keywords— **OSINT, *Phishing, Social Engineering, Auditing and Policy Based***