ABSTRACT

Phishing is an attack in which an attacker tries to obtain sensitive information such as personal data by posing as a trusted entity. Information security can be measured by testing phishing attacks. This study aims to mitigate information security based on the results of phishing attack experiments. Experiments using OSINT tools and social engineering activities by mitigating based on human-based methods. Phishing attacks are carried out using spear phishing and social media phishing techniques. Spear phishing is used to manipulate a field in a company by cloning the company's website url using SEToolkit, social media phishing with social media cloning websites, such as Instagram and Facebook using Zphisher, to company employees. The most dominant OSINT tool is Snov.io by obtaining 81 data on names, emails, and jobs. OSINT, social engineering, and phishing attack experiments are explained in the form of DFDs to show the flow of attacks carried out. Activity diagrams are used to formulate the use of email content. After obtaining the data, a comparative analysis of the results of the email content experiment is carried out to compile mitigation in order to prevent the impact of cyber attacks. Mitigation used using human-based methods, methods that focus on the people aspect, namely aspects that focus on human awareness and behavior to prevent the threat of phishing attacks. By providing education to employees routinely, at least once a month through training, simulations, and testing, companies can prevent the possibility of security incidents caused by employee negligence or lack of knowledge.

Keywords— ***phishing,*** **OSINT,** ***social engineering, human-based, mitigation***