ABSTRAK

Phishing merupakan serangan di mana penyerang mencoba untuk mendapatkan informasi sensitif seperti data pribadi dengan menyamar sebagai entitas yang terpercaya. Keamanan informasi dapat diukur dari pengujian *phishing attack*. Penelitian ini bertujuan untuk melakukan mitigasi terhadap keamanan informasi berdasarkan hasil eksperimen *phishing attack*. Eksperimen menggunakan OSINT *tools* dan aktivitas *social engineering* dengan melakukan mitigasi berdasarkan metode *human-based*. *Phishing attack* yang dilakukan menggunakan teknik spear phishing dan social media phishing. *Spear phishing* digunakan untuk memanipulasi suatu bidang pada perusahaan dengan cara *website cloning* url perusahaan dengan menggunakan SEToolkit, *social media phishing* dengan *website cloning* media sosial, seperti Instagram dan Facebook menggunakan Zphisher, kepada pegawai perusahaan. OSINT *tools* yang paling dominan adalah Snov.io dengan mendapatkan data nama, *email*, dan pekerjaan sebanyak 81 data. Eksperimen OSINT, *social engineering*, dan *phishing attack* dijelaskan dalam bentuk DFD untuk menunjukkan alur dari serangan yang dilakukan. *Activity diagram* digunakan untuk merumuskan penggunaan konten *email*. Setelah mendapatkan data, dilakukan analisis perbandingan dari hasil eksperimen konten *email* untuk menyusun mitigasi agar dapat mencegah dampak serangan siber. Mitigasi yang digunakan menggunakan metode *human-based*, metode yang berfokus pada aspek *people*, yaitu aspek yang berfokus pada kesadaran dan perilaku manusia untuk mencegah ancaman serangan *phishing*. Dengan memberikan edukasi kepada pegawai secara rutin, setidaknya sebulan sekali melalui pelatihan, simulasi, dan pengujian, perusahaan dapat mencegah kemungkinan terjadinya insiden keamanan yang disebabkan oleh kelalaian atau kurangnya pengetahuan pegawai.

Kata kunci— ***phishing,* OSINT, *social engineering, human-based,* mitigasi**