BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi informasi dan komunikasi yang sudah sangat berkembang di era industri 4.0 yang pesat membuka banyak fasilitas yang tersedia. Perkembangan teknologi informasi, termasuk Internet, komputasi awan, dan perangkat seluler, telah menciptakan lebih banyak pintu masuk ke sistem, memperluas serangan yang mungkin, dan meningkatkan kerentanannya. Ancaman terhadap keamanan informasi dapat berasal dari berbagai pihak, termasuk peretas, penjahat siber, pesaing, dan bahkan pegawai yang tidak bermaksud baik. Keamanan siber mencakup segala sesuatu berhubungan dengan pengawasan komputer, *monitoring* sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental (Budi et al., 2021). Dalam mencegah ancaman terhadap keamanan informasi suatu perusahaan, dapat dilakukan pengujian serangan *phishing* dengan menggunakan OSINT *tools* dan *social engineering* untuk menganalisis hasil dari pengujian agar dapat dilakukan mitigasi berdasarkan hasil analisis dari serangan *phishing* tersebut. Teknik yang dapat dipakai dalam pengujian serangan *phishing* tersebut, yaitu *spear phishing* dan *social media phishing. Spear phishing* untuk melakukan serangan dengan menargetkan suatu individu dan *social media phishing* untuk melakukan serangan menggunakan *website* media sosial yang sering dipakai target.

Seperti pada kasus yang ada di PT. XYZ yang terjadi kebocoran data. Berdasarkan kasus tersebut dapat dilakukan pengujian untuk menganalisis keamanan informasi dengan melakukan *phishing attack* menggunakan OSINT dan *social engineering*. OSINT sendiri berguna sebagai tempat pengumpulan data yang digunakan untuk menganalisis sumber informasi terbuka dan *social engineering* merupakan teknik untuk memanipulasi target agar dapat memberikan informasi pribadi. OSINT dapat digunakan untuk mengidentifikasi aktivitas yang mencurigakan, seperti pada kasus yang akan dibahas yaitu tentang kebocoran data pribadi pada suatu perusahaan.(Prasetyo et al., 2023). Sedangkan *social engineering* memanipulasi

individu dan perusahaan untuk membocorkan data berharga dan sensitif demi kepentingan penjahat dunia maya. (Salahdine & Kaabouch, 2019).

Dari hasil pengujian serangan tersebut dapat dilakukan mitigasi untuk mencegah dampak terkena serangan siber yang akan merugikan perusahaan dengan meningkatkan pemahaman terhadap bahaya serangan siber. Mitigasi pada penelitian ini menggunakan metode *human-based*. Metode *human-based* ini merupakan pendekatan yang memprioritaskan pengetahuan, sikap, dan tindakan yang dilakukan oleh manusia dalam upaya pengembangan sistem atau aplikasi.

I.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah:

1. Bagaimana implementasi *phishing attack* dalam mengidentifikasi keamanan informasi?
2. Bagaimana keterkaitan antara OSINT dan *social engineering* dalam menghasilkan serangan *phishing*?
3. Bagaimana menyusun mitigasi terhadap serangan *phishing*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengimplementasi *phishing attack* menggunakan teknik *spear phishing* dan *social media phishing*.
2. Menganalisa keterkaitan antara OSINT dan *social engineering* dalam melakukan serangan *phishing* pada organisasi dan *social media*.
3. Menyusun mitigasi menggunakan metode *human-based.*

I.4 Batasan Penelitian

Adapun batasan pada penelitian Tugas Akhir ini adalah sebagai berikut:

1. Penelitian ini tidak melibatkan eksploitasi atau pelaksanaan serangan.
2. Penelitian ini tidak melakukan *email spoofing*.
3. Penelitian ini tidak membahas praktik rinci dari mitigasi.

I.5 Manfaat Penelitian

1. Secara teoritis
    a. Penelitian ini bermanfaat dalam meningkatkan pemahaman tentang keamanan siber.
    b. Penelitian ini dapat menambah literatur mengenai OSINT, *social engineering*, dan *phishing attack*
2. Secara praktis,
    a. Penelitian ini bermanfaat untuk mengetahui mekanisme implementasi *phishing attack.*
    b. Penelitian ini bermanfaat untuk mengetahui langkah-langkah yang dapat dilakukan dalam proses pelatihan dan simulasi terhadap pegawai dalam mitigasi terkena serangan *phishing*.