BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam era digital ini, keamanan informasi dan kewaspadaan terhadap risiko kebocoran informasi merupakan aspek yang sangat penting dalam penggunaan teknologi informasi, terutama untuk data yang bersifat rahasia dan strategis. Setiap informasi harus dilindungi agar keamanan dan kerahasiaannya tetap terjaga dari berbagai ancaman, seperti akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan oleh pihak yang tidak berwenang (Pratiwi & Wulandari, 2021). Dalam menghadapi tantangan ini, *social engineering* menjadi salah satu teknik yang digunakan oleh pelaku kejahatan untuk memanfaatkan kelemahan manusia dalam sistem keamanan. Dengan menggunakan teknik manipulasi psikologis, mereka dapat menipu individu agar memberikan akses kepada informasi sensitif yang seharusnya dilindungi dengan baik.

Untuk menghadapi tantangan keamanan informasi, khususnya dalam menganalisis kebocoran data, penggunaan OSINT *tools* menjadi sangat relevan. OSINT digunakan untuk mengumpulkan dan menganalisis data dari sumber terbuka untuk mengidentifikasi potensi kebocoran data. Sebagai contoh, kasus kebocoran data pribadi pada PT. XYZ. OSINT dapat dimanfaatkan untuk melakukan aktivitas *social engineering* dengan cara mengumpulkan informasi dari sumber publik dan situs *web* perusahaan. Informasi yang dikumpulkan ini kemudian digunakan percobaan *phishing* dengan teknik *spear phishing* yang bertujuan untuk mengetahui tingkat kelemahan keamanan suatu perusahaan.

Perusahaan dapat menerapkan mitigasi risiko yang efektif dengan menggunakan metode *technology based* untuk menghadapi serangan *phishing*. Langkah ini bertujuan untuk memperkuat pertahanan perusahaan dan mencegah risiko terkena serangan *phishing*, sehingga keamanan data dan informasi perusahaan tetap terjaga dengan baik.

I.2 Perumusan Masalah

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

1. Bagaimana menyusun serangan *phishing attack* berdasarkan keterkaitan OSINT *tools* dan *social engineeirng*?
2. Bagaimana keterhubungan antara OSINT dan *social engineering* dalam melancarkan *phishing attack*?
3. Bagaimana merancang metode yang tepat untuk mitigasi risiko *phishing attack*?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang ada, tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Menyusun *phishing attack* dari OSINT *tools* dan *social engineering* berdasarkan teknik *spear phishing*.
2. Mengetahui keterhubungan antara implementasi *tools* OSINT dan *social engineering* untuk melancarkan *phishing attack.*
3. Merancang mitigasi risiko *phishing attack* yang tepat menggunakan metode *technology 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 mengimplementasikan praktik teknis dari filter *email* dan autentikasi dua faktor (2FA).

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
   a. Dapat memperkaya literatur mengenai penggunaan *tools* OSINT dan *phishing* dalam serangan *social enginering*.

b. Dapat menambah pemahaman terkait filter *email* dan autentikasi dua faktor (2FA) sebagai mitigasi risiko dengan metode *technology based*.

2. Secara praktis

   a. Memahami mekanisme praktis bagaimana *phishing attack* itu terjadi berdasarkan teknik *spear phishing*.
   b. Mengetahui pilihan teknologi yang digunakan untuk pencegahan *phishing attack*.