BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi internet yang semakin cepat telah memberikan dampak yang sangat signifikan bagi masyarakat global. Perkembangan tersebut telah mengubah berbagai aspek kehidupan menjadi lebih modern, mencakup bidang sosial, budaya, ekonomi, militer, administrasi, dan lainnya (Wahyudi & Sukmasari, 2018). Adanya perkembangan teknologi internet dan kemudahan akses informasi juga membuka peluang kejahatan yang dapat mengancam keamanan data dan informasi. Keamanan informasi merupakan aspek penting dari kemajuan teknologi informasi di era digital ini. Perlindungan data dan keamanan informasi juga merupakan kebutuhan untuk memastikan integritas, keamanan, dan ketersediaan informasi dalam suatu perusahaan.

Namun, meskipun upaya perlindungan data terus meningkat, kebocoran data tetap menjadi ancaman signifikan. Penggunaan OSINT dalam hal ini dapat membantu dalam menganalisis kebocoran data pada PT. XYZ dan mengidentifikasi celah keamanan yang mungkin perlu diperbaiki. OSINT dapat digunakan untuk melakukan aktivitas *social engineering* yaitu mengumpulkan informasi dari sumber publik dan situs *web* perusahaan.

Untuk menghadapi serangan *phishing*, dapat menerapkan mitigasi yang tepat yaitu menggunakan metode *auditing and policy-based* untuk memastikan bahwa perusahaan dapat memperkuat pertahanan dan mengurangi potensi serangan *phishing*. Mitigasi ini tidak hanya bergantung pada teknologi, tetapi juga melibatkan *auditing* yang sistematis serta kebijakan yang tepat untuk menjaga keamanan data dalam menghadapi serangan *phishing*.

I.2 Perumusan Masalah

Berdasarkan uraian masalah yang telah dijelaskan pada latar belakang, maka permasalahan yang akan dikaji pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara menerapkan teknik yang tepat dalam implementasi *phishing attack* untuk mengetahui keamanan informasi?
2. Bagaimana hubungan antara OSINT dan aktivitas *social engineering* untuk melakukan *phishing attack?*
3. Bagaimana metode yang tepat dan dapat diterapkan untuk mitigasi *phishing attack*?

I.3 Tujuan Penelitian

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

1. Menerapkan teknik *spear phishing* dalam implementasi *phishing attack.*
2. Mengetahui hubungan antara implementasi OSINT *tools* dan aktivitas *social engineering* untuk melakukan *phishing attack.*
3. Menyusun metode *auditing and policy-based* yang tepat untuk mitigasi *phishing attack.*

I.4 Batasan Penelitian

Adapun batasan dalam melakukan penelitian ini, sebagai berikut:

1. Penelitian ini tidak melibatkan eksploitasi atau pelaksaan serangan.
2. Penelitian ini tidak melakukan *email spoofing*.
3. Penelitian ini tidak melakukan praktik implementasi mitigasi.

I.5 Manfaat Penelitian

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

1. Secara teoritis
    a. Memperluas pemahaman mengenai tools OSINT *tools* dan *Phishing* dalam mengidentifikasi kerentanan keamanan informasi melalui aktivitas *social engineering* dan teknik *email spear phishing*.
    b. Mengembangkan model teoritis yang menunjukkan bagaimana metode *auditing and policy-based* terhadap keamanan dapat digunakan untuk mitigasi serangan *phishing*.
2. Secara praktis
    a. Membantu perusahaan memahami dan mengantisipasi aktivitas *social engineering* dan *phishing attack*, untuk menerapkan langkah pencegahan yang lebih tepat.
    b. Menyediakan rekomendasi mitigasi untuk metode *auditing and policy based* terhadap keamanan yang dapat diimplementasikan oleh perusahaan untuk mengurangi serangan *phishing*.