BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang terus berkembang, serangan siber, khususnya ***phishing attack***, menjadi salah satu ancaman terbesar bagi keamanan informasi perusahaan. *Phishing* adalah metode yang digunakan oleh pelaku kejahatan siber untuk mencuri data sensitif seperti kredensial login, informasi keuangan, atau data rahasia perusahaan melalui email, pesan teks, atau situs web palsu. Laporan dari *Verizon Data Breach Investigations Report 2023* menunjukkan bahwa lebih dari 36% pelanggaran data dimulai dari serangan *phishing*, menjadikannya salah satu vektor serangan utama di berbagai industri [1].

Phishing tidak hanya berdampak pada hilangnya data penting, tetapi juga berpotensi merugikan perusahaan secara finansial dan reputasi. Menurut penelitian dari *IBM Security X-Force*, biaya rata-rata pelanggaran data akibat serangan *phishing* mencapai USD 4,91 juta pada tahun 2023. Hal ini menunjukkan pentingnya pengelolaan keamanan siber yang efektif untuk meminimalkan risiko tersebut [2].

Sebagai perusahaan yang bergerak di industri jasa keuangan, PT. Infogram Telemedia menghadapi tantangan besar dalam menjaga keamanan data perusahaan, terutama karena tingginya tingkat ancaman *phishing* yang ditujukan pada sektor ini. Laporan dari *Anti-Phishing Working Group (APWG)* menyebutkan bahwa sektor jasa keuangan adalah salah satu target utama serangan *phishing* global, dengan lebih dari 20% serangan menyasar perusahaan di bidang ini pada tahun 2023.

Untuk mengatasi ancaman tersebut, PT. Infogram Telemedia mengimplementasikan platform keamanan *KnowBe4*, yang dirancang untuk meningkatkan kesadaran karyawan terhadap ancaman siber melalui pelatihan keamanan interaktif dan simulasi *phishing*. Platform ini juga dilengkapi dengan fitur seperti **Phish Alert Button (PAB)** untuk membantu mendeteksi dan melaporkan email mencurigakan dengan mudah. Implementasi ini diharapkan dapat mengurangi risiko kesalahan manusia (*human error*), yang sering menjadi penyebab utama keberhasilan serangan *phishing*.

Latar belakang ini menunjukkan bahwa implementasi solusi keamanan seperti *KnowBe4* bukan hanya langkah preventif, tetapi juga strategis dalam

melindungi integritas dan keberlanjutan operasi perusahaan di tengah meningkatnya ancaman siber global.

1.2 Maksud dan Tujuan Kerja Magang

1.2.1 Maksud Kerja Magang

Tujuan mengikuti program magang ini adalah untuk memenuhi salah satu persyaratan kelulusan akademis, serta sebagai peluang berharga dalam mengembangkan diri dan memperoleh pengalaman langsung di industri teknologi.

1.2.2 Tujuan Kerja Magang

Tujuan dari program magang ini adalah untuk memberikan pengalaman praktis kepada peserta dalam bidang teknologi informasi, khususnya pada peran sebagai *System Security Engineer*, guna mendukung keamanan dan operasional sistem di PT. Infogram Telemedia. Dalam program ini, peserta tidak hanya mempelajari penerapan solusi teknologi di industri keuangan, seperti *Core Banking System* dan *Electronic Fund Transfer (EFT) Switching and Card Management System*, tetapi juga berfokus pada implementasi platform keamanan KnowBe4. Platform ini digunakan untuk meningkatkan kesadaran keamanan (*security awareness*) karyawan melalui pelatihan interaktif dan simulasi serangan siber, yang menjadi bagian penting dalam strategi perusahaan untuk memperkuat postur keamanan siber serta memitigasi risiko ancaman yang berkembang. [3] .

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Periode pelaksanaan magang pada PT. Infogram Telemedia berlangsung selama enam bulan yang dimulai pada 22 Agustus 2024 hingga 28 Februari 2025. Jadwal pelaksanaan magang pada PT. Infogram Telemedia adalah Senin sampai Jumat, dengan jam kerja 9 jam setiap harinya. Peserta magang akan dilibatkan dalam kegiatan sesuai dengan produk yang ditugaskan untuk memberikan pengalaman nyata dan meningkatkan pemahaman mengenai dunia kerja. Lokasi kerja magang berada di Menara Batavia 22nd Floor Jl. K.H. Mansyur Kav. 126 Jakarta Pusat, 10220 , serta akan dibimbing oleh supervisor terlebih dahulu dan akan diserahkan ke tim leader atau PIC produknya masing-masing. Peserta juga diharapkan untuk mematuhi prosedur dan peraturan yang

berlaku di lingkungan kerja tersebut dan juga menyelesaikan tugas-tugas yang telah ditetapkan sesuai dengan jadwal yang telah ditentukan. Melalui pengalaman magang ini, diharapkan peserta magang akan dapat mengembangkan keterampilan dan pengetahuan yang relevan dengan bidang pekerjaan.