BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Magang

Kerja Praktek (KP) merupakan kegiatan yang dilakukan sesuai dengan pemahaman dan konsep ilmu pengetahuan yang diaplikasikan dalam pekerjaan sesuai profesi bidang studi. Kerja praktek dilakukan untuk meningkatkan ilmu sosial, pengetahuan, dan keahlian mahasiswa. Untuk memasuki dunia kerja setelah kuliah, mahasiswa harus memiliki pengalaman sebelumnya. Pengetahuan ilmu teori yang diperoleh selama kuliah belum tentu sama dengan praktik nyata di lapangan. Kerja praktek memungkinkan mahasiswa untuk terhubung dengan dunia industri dan instansi, mengintegrasikan pengetahuan akademis dengan pengalaman praktis.

Program Studi Keamanan Sistem Informasi merupakan salah satu program studi yang ada di Politeknik Negeri Bengkalis. Program studi ini mempelajari bidang keamanan teknologi informasi, mencakup berbagai aspek seperti keamanan jaringan, analisis ancaman siber, serta pengelolaan sistem informasi secara aman dan terstandar. Program Studi Keamanan Sistem Informasi mengharuskan mahasiswa menyelesaikan kerja praktek untuk meningkatkan pemahaman mereka tentang keamanan siber secara praktis, sehingga menghasilkan lulusan yang berkualitas dan memiliki pengalaman kerja yang relevan dengan industri.

Kerja praktek yang dilaksanakan di Bank Riau Kepri Syariah merupakan salah satu tempat pelaksanaan kerja praktek yang sesuai dengan bidang studi Keamanan Sistem Informasi. Bank Riau Kepri Syariah merupakan salah satu bank daerah milik Pemerintah Provinsi Riau dan Kepulauan Riau yang bergerak di bidang layanan perbankan berbasis syariah. Bank Riau Kepri Syariah memberikan kesempatan kepada mahasiswa untuk melaksanakan Kerja Praktek (KP) guna meningkatkan kualitas dan wawasan yang dimiliki, khususnya di bidang keamanan sistem informasi. Di samping

itu, Bank Riau Kepri Syariah juga memberikan tugas sesuai dengan profesi bidang studi mahasiswa yang melaksanakan kerja praktek.

Dalam mendukung keamanan sistem informasi, Bank Riau Kepri Syariah menggunakan tools keamanan seperti IBM QRadar sebagai platform Security Information and Event Management (SIEM). IBM QRadar digunakan untuk membantu proses pengumpulan log, korelasi event, monitoring aktivitas keamanan, serta deteksi potensi ancaman pada sistem yang terhubung. Penggunaan tools SIEM tersebut sangat penting di lingkungan perbankan karena dapat membantu tim keamanan dalam memantau aktivitas sistem secara terpusat, mendeteksi anomali, dan mendukung proses investigasi insiden keamanan siber.

Selama pelaksanaan kerja praktek di Bank Riau Kepri Syariah, penulis ditempatkan pada Divisi Teknologi & Sistem Informasi dan mendapatkan kesempatan untuk memanfaatkan Wazuh SIEM sebagai sistem deteksi dan monitoring ancaman keamanan siber. Alasan penulis mengangkat topik ini adalah karena penulis diberikan tugas oleh Divisi Teknologi & Sistem Informasi Bank Riau Kepri Syariah untuk melakukan monitoring keamanan jaringan menggunakan Wazuh SIEM berbasis *MITRE ATT&CK Framework*, sehingga topik ini sangat relevan dengan bidang studi Keamanan Sistem Informasi yang sedang ditempuh.

1.2 Tujuan dan Manfaat Magang

1.2.1 Tujuan Magang

Kegiatan magang yang dilaksanakan di Divisi Teknologi & Sistem Informasi Bank Riau Kepri Syariah memiliki tujuan sebagai berikut:

1. Memahami secara langsung pemanfaatan Wazuh SIEM sebagai sistem deteksi dan monitoring ancaman keamanan siber di lingkungan perbankan nyata, mulai dari cara kerja sistem, konfigurasi yang diterapkan, hingga proses analisis alert yang dihasilkan secara real-time.

2. Mempelajari dan menerapkan *MITRE ATT&CK Framework* sebagai kerangka kerja standar internasional dalam mengklasifikasikan, menganalisis, dan memetakan ancaman keamanan siber yang terdeteksi oleh Wazuh SIEM ke dalam teknik serangan yang terdokumentasi secara ilmiah.
3. Mengembangkan kemampuan analisis log dan investigasi insiden keamanan siber secara praktis, sehingga mahasiswa mampu mengidentifikasi, mengklasifikasikan, dan mendokumentasikan ancaman yang ditemukan selama kegiatan monitoring berlangsung di lingkungan kerja yang sesungguhnya.
4. Melakukan wawancara dengan pembimbing lapangan di Divisi Teknologi & Sistem Informasi untuk memperoleh informasi terkait prosedur kerja, sistem keamanan yang digunakan, pemanfaatan tools SIEM seperti IBM QRadar dan Wazuh SIEM, serta kebijakan keamanan informasi yang diterapkan di lingkungan PT Bank Riau Kepri Syariah.
5. Memenuhi persyaratan akademik Program Studi Sarjana Terapan Keamanan Sistem Informasi Politeknik Negeri Bengkalis sebagai bagian dari kurikulum yang mewajibkan mahasiswa untuk menjalani kegiatan magang di industri guna mendapatkan pengalaman kerja yang nyata dan relevan dengan bidang studinya.

1.2.2 Manfaat Magang

Kegiatan magang ini diharapkan memberikan manfaat bagi tiga pihak, yaitu mahasiswa, instansi tempat magang, dan perguruan tinggi.

1. Bagi Mahasiswa
    a. Mendapatkan pengalaman kerja langsung di bidang keamanan siber perbankan, khususnya dalam pengoperasian dan pemanfaatan Wazuh SIEM sebagai tools profesional yang banyak digunakan di industri.
    b. Meningkatkan pemahaman dan kemampuan dalam menganalisis log keamanan, mendeteksi ancaman siber, serta memetakan temuan ke dalam

kerangka kerja *MITRE ATT&CK Framework* secara sistematis dan terstandar.

c. Menjembatani kesenjangan antara teori keamanan sistem informasi yang dipelajari di bangku perkuliahan dengan praktik nyata di dunia kerja, sehingga mahasiswa siap bersaing di industri keamanan siber yang terus berkembang.

2. Bagi Bank Riau Kepri Syariah

a. Mendapatkan kontribusi tenaga dari mahasiswa magang dalam kegiatan monitoring dan analisis keamanan siber harian, sehingga dapat membantu meringankan beban kerja tim Divisi Teknologi & Sistem Informasi dalam mengawasi aktivitas jaringan dan sistem secara berkelanjutan.

b. Memperoleh masukan dan dokumentasi teknis terkait pemanfaatan Wazuh SIEM berbasis *MITRE ATT&CK Framework* yang dapat dijadikan referensi dalam pengembangan dan peningkatan sistem keamanan siber bank ke depannya.

1.3 Luaran Proyek Magang

Selama melakukan proyek yang diberikan pada saat kerja praktek, adapun pekerjaan yang dilakukan selama di Bank Riau Kepri Syariah yaitu berupa pemanfaatan Wazuh SIEM untuk deteksi dan monitoring ancaman keamanan siber berbasis *MITRE ATT&CK Framework.*