BAB I
PENDAHULUAN

1.1. Latar Belakang Pemikiran Magang

Magang atau Kerja Praktek merupakan serangkaian kegiatan yang meliputi pemahaman teori atau konsep ilmu pengetahuan yang diaplikasikan dalam pekerjaan sesuai profesi bidang studi. Kegiatan ini dapat menambah wacana, pengetahuan dan skill mahasiswa, serta mampu menyelesaikan persoalan persoalan ilmu pengetahuan sesuai dengan teori yang mereka peroleh di perkuliahan. Magang dilaksanakan agar mahasiswa dapat memahami dan menerapkan secara baik tentang bidang ilmu yang dipelajari pada dunia industri, dunia usaha dan dunia kerja (IDUKA). Selain itu, agar mahasiswa dapat mengetahui profesi serta atmosfir pekerjaan sesuai dengan program studinya.

Program studi Keamanan Sistem Informasi merupakan program studi yang ada di kampus Politeknik Negeri Bengkalis. Program studi ini menekankan pada perlindungan data, sistem jaringan, serta pengelolaan risiko digital. Mahasiswa Keamanan Sistem Informasi dituntut untuk tidak hanya memahami teori keamanan, tetapi juga mampu melihat dan menerapkan sistem pertahanan digital dalam lingkungan kerja yang sebenarnya. Whitman dan Mattord menjelaskan bahwa implementasi keamanan informasi dalam suatu organisasi merupakan proses yang dilakukan secara bertahap (*incremental process*) dan memerlukan koordinasi, waktu, serta dukungan organisasi agar dapat berjalan secara efektif. Oleh karena itu, pengalaman langsung melalui kerja praktik menjadi sarana bagi mahasiswa untuk mengembangkan kemampuan analisis terhadap penerapan keamanan sistem informasi berdasarkan kondisi nyata yang ditemukan di lingkungan industri.

PT XYZ merupakan perusahaan yang bergerak di bidang manufaktur dan pengolahan kelapa sawit yang menghasilkan berbagai produk turunan seperti biodiesel, minyak goreng, dan produk berbasis minyak sawit lainnya. Dalam mendukung aktivitas operasionalnya, perusahaan memanfaatkan berbagai infrastruktur teknologi informasi yang meliputi jaringan komputer, server,

perangkat penyimpanan data, sistem informasi, serta mekanisme pengelolaan dan pencadangan (*backup*) data untuk mendukung keberlangsungan proses bisnis perusahaan. Penulis memilih PT XYZ sebagai tempat pelaksanaan kerja praktik karena perusahaan memiliki lingkungan teknologi informasi yang kompleks sehingga memberikan kesempatan untuk mempelajari penerapan keamanan sistem informasi secara langsung pada lingkungan industri.

Selama pelaksanaan kerja praktik, penulis ditempatkan pada tim *IT Support* yang bertanggung jawab terhadap pengelolaan infrastruktur teknologi informasi perusahaan. Ruang lingkup pekerjaan tim meliputi pengelolaan perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komputer, server, perangkat penyimpanan data, serta berbagai perangkat pendukung lainnya agar seluruh layanan teknologi informasi dapat beroperasi secara optimal dalam mendukung aktivitas perusahaan. Selain terlibat secara langsung dalam berbagai kegiatan operasional, penulis juga melakukan observasi terhadap proses pengelolaan infrastruktur teknologi informasi yang diterapkan oleh perusahaan. Melalui kegiatan tersebut, penulis memperoleh pemahaman bahwa selain pengelolaan jaringan dan server, perusahaan juga menerapkan mekanisme *backup* data sebagai bagian dari upaya menjaga keberlangsungan operasional teknologi informasi. Salah satu media yang digunakan dalam proses *backup* tersebut adalah *tape server*, yang berfungsi sebagai media penyimpanan cadangan data perusahaan. Hasil observasi tersebut menjadi dasar bagi penulis untuk melakukan analisis terhadap penerapan keamanan dalam pengelolaan media *backup* data *tape server* berdasarkan prinsip *Confidentiality, Integrity,* dan *Availability* (*CIA Triad*) sebagai fokus pembahasan dalam laporan kerja praktik ini.

Data merupakan salah satu aset yang paling penting bagi organisasi karena mendukung berbagai aktivitas operasional maupun proses pengambilan keputusan. *Whitman* dan *Mattord* menjelaskan bahwa data yang disimpan, diproses, maupun ditransmisikan oleh sistem komputer harus memperoleh perlindungan yang memadai karena merupakan aset organisasi yang bernilai tinggi dan menjadi sasaran utama berbagai ancaman keamanan informasi [3].

Salah satu upaya yang dapat dilakukan untuk melindungi data adalah dengan menerapkan mekanisme *backup* secara berkala. Melalui proses *backup*, organisasi memiliki salinan data yang dapat digunakan kembali apabila terjadi gangguan pada sistem utama atau ketika diperlukan proses pemulihan data. NIST menjelaskan bahwa *backup* berperan sebagai bagian dari fungsi *Recover*, sehingga salinan data harus dibuat sebelum terjadinya suatu insiden agar dapat dimanfaatkan dalam proses pemulihan sistem. Selain itu, pelaksanaan dan konfigurasi *backup* perlu disesuaikan dengan kebutuhan operasional serta tingkat risiko yang dimiliki oleh organisasi.

Media *backup* tidak hanya berfungsi sebagai tempat penyimpanan salinan data, tetapi juga menyimpan informasi yang memiliki nilai penting bagi organisasi. Oleh karena itu, pengelolaan media *backup* tidak hanya berorientasi pada keberhasilan proses pencadangan (*backup*) dan pemulihan (*recovery*) data, tetapi juga perlu memperhatikan aspek keamanan terhadap data yang tersimpan di dalamnya. Pengelolaan yang baik diperlukan untuk memastikan bahwa data cadangan tetap terlindungi dari akses yang tidak berwenang, perubahan data yang tidak sah, maupun kehilangan data yang dapat memengaruhi operasional organisasi. Dengan demikian, keamanan dalam pengelolaan media *backup* menjadi salah satu aspek penting yang perlu diperhatikan agar data cadangan tetap dapat memberikan perlindungan dan mendukung keberlangsungan sistem informasi perusahaan.

Untuk menganalisis aspek keamanan dalam pengelolaan media *backup* data, diperlukan suatu kerangka yang dapat digunakan sebagai dasar evaluasi. Salah satu konsep yang banyak digunakan dalam bidang keamanan informasi adalah *CIA Triad*. *National Institute of Standards and Technology (NIST)* menjelaskan bahwa *CIA Triad* merupakan tiga pilar utama keamanan informasi (*the three pillars of information security*), yang terdiri atas *Confidentiality*, *Integrity*, dan *Availability*. Prinsip *Confidentiality* bertujuan menjaga pembatasan akses dan pengungkapan informasi agar hanya dapat diakses oleh pihak yang berwenang. Prinsip *Integrity* bertujuan melindungi informasi dari perubahan atau kerusakan yang tidak sah serta menjaga keaslian informasi, sedangkan prinsip *Availability* bertujuan memastikan informasi dapat diakses dan digunakan secara tepat waktu serta andal oleh pihak

yang berwenang. Oleh karena itu, penelitian ini menggunakan prinsip *CIA Triad* sebagai kerangka analisis untuk mengevaluasi keamanan pengelolaan media *backup* data *tape server* di PT XYZ.

Berdasarkan hasil observasi selama pelaksanaan kerja praktik, pengelolaan media *backup* data *tape server* merupakan salah satu bagian penting dalam mendukung perlindungan aset informasi perusahaan. Oleh karena itu, diperlukan suatu analisis untuk mengetahui bagaimana penerapan prinsip *Confidentiality*, *Integrity*, dan *Availability* dalam pengelolaan media *backup* data tersebut sehingga dapat memberikan gambaran mengenai penerapan aspek keamanan informasi di lingkungan perusahaan. Berdasarkan uraian tersebut, penulis mengangkat laporan kerja praktik dengan judul **"Analisis Keamanan Pengelolaan Media *Backup Data Tape* Server Berdasarkan Prinsip *CIA Triad* di PT XYZ."**

1.2.Tujuan dan Manfaat Magang

Adapun tujuan dari pelaksanaan magang ini adalah sebagai berikut:

1. Memenuhi persyaratan akademik program studi sebagai bagian dari kurikulum yang wajib ditempuh oleh mahasiswa.
2. Memperoleh pengalaman kerja secara langsung di lingkungan industri melalui pelaksanaan kerja praktik pada Divisi *IT Support* PT XYZ.
3. Memahami proses pengelolaan infrastruktur teknologi informasi perusahaan, meliputi server, jaringan komputer, perangkat penyimpanan data, serta media *backup* yang digunakan dalam mendukung operasional perusahaan.
4. Menerapkan pengetahuan dan keterampilan yang diperoleh selama perkuliahan ke dalam aktivitas kerja nyata di bidang teknologi informasi.
5. Menganalisis penerapan prinsip *Confidentiality*, *Integrity*, dan *Availability* dalam pengelolaan media *backup* data *tape server* sebagai bagian dari penerapan keamanan sistem informasi di PT XYZ.

Sedangkan manfaat yang ingin diperoleh dari pelaksanaan magang ini adalah sebagai berikut:

1. Memperoleh pengalaman kerja secara langsung di lingkungan industri, khususnya pada bidang pengelolaan infrastruktur teknologi informasi.

2. Menambah pemahaman mengenai proses pengelolaan server, jaringan komputer, media *backup* data, serta perangkat pendukung lainnya yang digunakan di lingkungan perusahaan.
3. Meningkatkan kemampuan teknis dalam pengelolaan infrastruktur teknologi informasi berdasarkan praktik yang diterapkan di dunia industri.
4. Mengembangkan kemampuan bekerja sama, berkomunikasi, serta beradaptasi dengan budaya kerja profesional di lingkungan perusahaan.
5. Menambah wawasan mengenai pentingnya pengelolaan media *backup* data sebagai bagian dari upaya menjaga keberlangsungan operasional sistem informasi.
6. Memahami penerapan prinsip *Confidentiality*, *Integrity*, dan *Availability* dalam pengelolaan media *backup* data sebagai bagian dari keamanan sistem informasi.
7. Memperoleh pengalaman dalam melakukan observasi dan analisis terhadap pengelolaan media *backup* data yang dapat dijadikan dasar penyusunan laporan kerja praktik.

1.3. Luaran Proyek Magang

Selama pelaksanaan kerja praktik di PT XYZ, penulis terlibat secara langsung dalam kegiatan operasional pengelolaan media *backup* data *tape server* pada Divisi *IT Support*. Kegiatan tersebut meliputi proses penggantian media *backup* (*tape*), pemberian label identitas berupa tanggal pelaksanaan *backup*, serta penyimpanan media *backup* sesuai dengan prosedur yang diterapkan oleh perusahaan. Pemberian label dilakukan untuk memudahkan proses identifikasi dan penelusuran data *backup*, sedangkan penyimpanan media *backup* dilakukan secara terstruktur berdasarkan kelompok data yang dikelola oleh perusahaan.

Pengelolaan media *backup* dilakukan dengan mengelompokkan setiap media *tape* berdasarkan unit atau entitas perusahaan yang berada dalam satu kawasan operasional. Pengelompokan tersebut bertujuan untuk mempermudah proses administrasi, penyimpanan, serta penelusuran kembali media *backup* apabila diperlukan dalam proses pemulihan (*recovery*) data. Selain itu, pemberian label dan pengelompokan media *backup* juga membantu meminimalkan risiko kesalahan

dalam penggunaan media *backup* serta mendukung pengelolaan arsip *backup* yang lebih teratur.

Melalui keterlibatan dalam kegiatan tersebut, penulis memperoleh pengalaman mengenai proses pengelolaan media *backup* data yang diterapkan di lingkungan perusahaan. Pengalaman tersebut menjadi dasar dalam penyusunan laporan kerja praktik yang mengkaji keamanan pengelolaan media *backup* data *tape server* berdasarkan prinsip *Confidentiality*, *Integrity*, dan *Availability* (*CIA Triad*). Hasil analisis yang disusun diharapkan dapat memberikan gambaran mengenai penerapan aspek keamanan informasi dalam pengelolaan media *backup* data di PT XYZ.