

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Informasi maupun data di era informasi seperti saat ini sudah menjadi hal yang sangat berharga. Bahkan kita bisa katakan sangat vital sehingga kerusakan, ataupun kebocoran terhadap informasi suatu organisasi dapat mengakibatkan organisasi tersebut berhenti atau tutup. Dikarenakan begitu berharganya suatu informasi atau data maka tidaklah heran jika kemudian bermunculan beberapa pihak yang tidak bertanggung jawab dimana pihak tersebut berusaha mencuri maupun merusak dan mengubah data atau informasi dari sistem komputer yang dimiliki oleh suatu organisasi tertentu, apakah itu untuk kesenangan individual atau sekelompok orang, oleh karena itu dibutuhkan keamanan sistem informasi yang terjamin bahwa sistem kita aman.

Ancaman itu sendiri bisa berasal dari ancaman luar, dalam, tak terstruktur, dan ancaman yang terstruktur (CCNA Security, Chapter 1). Mengamankan keamanan informasi bisa dimulai dengan mencegah serangan dari dalam, dikarenakan juga bahwa serangan yang berasal dari dalam lebih sering terjadi dan lebih berbahaya.

*Control A.11.4.4 ISO/IEC 27001:2005* membahas tentang pengamanan dari dalam, khususnya bagaimana mengamankan perangkat-perangkat jaringan yang terdapat dari sistem dari segi akses fisik ataupun logikal dari orang-orang

yang tidak berwenang mengaksesnya. Penelitian kali ini akan dicoba pada jaringan yang terdapat pada STMIK Amikom Yogyakarta.

## 1.2 Perumusan Masalah

STMIK Amikom Yogyakarta merupakan salah satu perguruan tinggi di Yogyakarta yang lagi sedang berkembang. Perguruan tinggi ini memiliki sistem informasi akademik yang menghubungkan setiap komputer dengan *server* yang terdapat pada area atau lingkungan kampus sehingga mahasiswa, dosen, karyawan dan lainnya bisa saling terhubung.

Dengan semakin berkembangnya sistem yang ada, terkadang keamanan informasi dapat diabaikan. Meskipun dampaknya tidak terlalu kelihatan, namun lama-kelamaan, ini akan menjadi masalah yang besar di kemudian hari, dan untuk memulihkan kembali sistem yang ada sebelum terjadi ancaman akan memerlukan waktu yang banyak dan membuat pelayanan terganggu.

Memperhatikan rincian masalah diatas, maka dapat diambil rumusan masalahnya yaitu pengamanan keamanan informasi dengan mengamankan perangkat-perangkat jaringan yang digunakan pada akses fisik dan logikal berdasarkan ISO/IEC 27001:2005 standar A.11.4.4.

## 1.3 Batasan Masalah

Terdapat 11 *control* pada ISO/IEC 27001:2005, namun peneliti membatasi dengan hanya mengambil satu *control* saja, pada standar A.11.4.4 (*Remote diagnostic and configuration port protection*), sehingga bagaimana mengamankan

sistem jaringan STMIK Amikom Yogyakarta dengan berdasarkan pada ISO/IEC 27001:2005 standar A.11.4.4.

#### **1.4 Tujuan Penelitian**

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Sebagai persyaratan untuk kelengkapan dalam program studi Strata 1 Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Amikom Yogyakarta.
2. Untuk membantu dalam pengamanan akses fisik dan logikal pada perangkat-perangkat jaringan yang digunakan dalam jaringan STMIK Amikom Yogyakarta seperti *router*, *switch*, dan sebagainya.

#### **1.5 Manfaat Penelitian**

Dari penelitian ini diharapkan dapat memberikan manfaat yaitu:

1. Sebagai referensi atau acuan dalam penerapan sistem keamanan akses fisik dan logikal pada perangkat jaringan.
2. Penyerang ataupun orang yang tidak berwenang tidak dapat mengakses perangkat-perangkat jaringan di STMIK Amikom Yogyakarta.

#### **1.6 Metode Penelitian**

Penulis melakukan beberapa penelitian dengan :

### 1. Studi Pustaka (Literatur)

Yaitu metode pencarian data dari buku, jurnal, internet atau literatur lainnya yang berkaitan dengan teori dasar yang berhubungan dengan penelitian.

### 2. Studi Sistem

Yaitu metode pencarian data dengan melakukan pengamatan langsung di lapangan.

## 1.7 Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan diuraikan dalam bentuk bab, dan masing-masing bab akan diuraikan lagi beberapa sub bab, diantaranya:

#### **BAB I. Pendahuluan**

Bab ini akan membahas latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penelitian.

#### **BAB II. Landasan Teori**

Dalam bab ini membahas teori-teori yang menjadi landasan dan mendukung pelaksanaan penulisan penelitian.

#### **BAB III. Metodologi Penelitian**

Dalam bab ini membahas tentang bagaimana langkah-langkah pengamanan perangkat jaringan dengan berdasarkan pada ISO/IEC 27001:2005 standar A.11.4.4.

#### **BAB IV. Implementasi dan Pembahasan**

Dalam bab ini akan dibahas dan dianalisa hasil penelitian yang telah dilakukan.

#### **BAB V. Punutup**

Dalam bab ini akan disampaikan kesimpulan dan saran.

