Southern New Hampshire University

CYB 220 Project Three Scenario One

The design of the protection of information technology (IT) systems requires evaluation of different components of the overall system. Below is the beginning of an organizational security plan that documents the general areas of relevance to your evaluation of network protection technologies.

Current Issue: In a series of incidents, people in acquisitions have tried to access the human resources network segment and it has slowed network communications. Individuals in information technology are trying to determine who is attempting unauthorized access. Your role is to help determine which type of intrusion detection system (IDS) or intrusion prevention system (IPS) to recommend. When considering which options to implement, you know that the IT department of the company consists of you and four other people, two of whom are new to IT and fresh out of college.

I. **General System Description/Purpose**

A. **System Description (Who)**

1. It is a financial institution.
2. There are 150 to 200 employees.
3. Company has been in business for over 20 years.
4. The institution has over 75 clients.

B. **System Architecture (What)**

1. Each employee has a host computer.
2. Network is broken up into four segments, with restricted access between the segments.
3. There is one segment for each of the different departments: sales, acquisitions, human resources (HR), and IT.
4. Remote availability for the IT segment is a necessity.

C. **Functional Architecture (How)**

1. The clients need availability to access their company information at any given time.
2. System maintenance is only performed weekly and done on Sunday nights.
3. Changes need to be implemented in the shortest amount of time.
4. The preference for the company is to use open-source (free) tools as solutions first.
5. There is a need to identify anyone with malicious intent.

D. **User Roles and Access Privileges**

1. The HR and IT departments are responsible for the protection and access of private information of individuals.
2. There is no need for any other department to access HR data.
3. There is no need for people to go outside their own network segment except IT.