|  |
| --- |
| Cyb 220 |
| Project Three Submission |
| Evaluation of Network Protection Technologies |

|  |
| --- |
| Zeppelin041  4-11-2023 |

1. Explain how you are employing one of the **Fundamental Security Design Principles** to inform your recommendation.

One of the fundamental security design principles that can be employed to inform the recommendation of IDS/IPS for the corporation is the principle of defense-in-depth. The defense-in-depth principle suggests that multiple layers of security controls should be used to protect assets from various types of attacks and security threats. In this scenario, the company suspects that someone is tampering with either the purchase transactions or the logging of inventory changes. To mitigate this threat, the company can implement multiple layers of IDS/IPS to detect and prevent unauthorized access to its systems and data. For example, the company can implement network-based IDS/IPS at the perimeter of its network to monitor incoming and outgoing traffic for suspicious activity. Host-based IDS/IPS can also be installed on individual retail store systems to monitor activity at the endpoint level. Additionally, the company can implement log analysis and correlation tools to detect and analyze anomalies in system logs and identify potential threats. These layers of security controls can provide a defense-in-depth approach to mitigating the threat of tampering with purchase transactions or inventory changes.

1. Justify a **recommended network protection approach**. Describe how you balanced effectiveness, cost, and technical capabilities to select the network protection technology.

One recommended network protection approach for the scenario described above is to implement a combination of network-based firewalls and intrusion prevention systems (IPS) to protect the company's network. Network-based firewalls can provide a first line of defense by monitoring and filtering incoming and outgoing traffic based on predefined rules and policies. This can help prevent unauthorized access to the network and block known threats before they can reach the company's systems and data. Intrusion prevention systems (IPS) can provide a more advanced level of network protection by monitoring network traffic in real-time, detecting and preventing known and unknown threats. IPS can also provide additional security features such as deep packet inspection, signature-based detection, and behavior-based detection, which can help identify and prevent sophisticated attacks that may bypass traditional firewall protections. When selecting the network protection technology, the company should consider several factors such as effectiveness, cost, and technical capabilities such as:

-**Effectiveness**: Network protection technology should be able to provide adequate protection against known and unknown threats while also minimizing false positives and negatives. The combination of firewalls and IPS can provide a layered approach to network protection that can help increase the effectiveness of the security measures.

-**Cost**: The company should consider the costs associated with implementing and maintaining the network protection technology. Network-based firewalls are generally less expensive than IPS, and they can provide a basic level of network protection. IPS, on the other hand, can be more expensive, but they provide more advanced network protection features.

-**Technical capabilities**: The company should consider the technical capabilities of the network protection technology, including features such as ease of deployment, management, and scalability. The network protection technology should be easy to deploy and manage, and it should be able to scale to meet the needs of the company as it grows.

1. **Recommend resources** that are necessary for implementing or monitoring your chosen network protection approach.

The following resources to implement and monitor the recommended network protection approach of network-based firewalls and intrusion prevention systems are:

1. **Organizational assets**: The company should have a dedicated security team or a security specialist who can oversee the implementation and monitoring of the network protection technology. The security team can develop and maintain security policies and procedures, oversee risk assessments, and conduct regular security audits.
2. **Workforce allocation**: The company should allocate resources to the security team or specialist to ensure that they have sufficient time and resources to manage and monitor the network protection technology effectively. Additionally, the company should consider training the workforce in best practices for network security and the use of the network protection technology.
3. **Policies/procedures**: The company should have clear policies and procedures for the deployment, configuration, and management of the network protection technology. These policies should outline the roles and responsibilities of the security team, the procedures for handling security incidents, and the process for updating security policies and procedures.
4. **Hardware**: The company should invest in hardware that can support network protection technology, such as high-performance firewalls and intrusion prevention systems. The hardware should be scalable to meet the needs of the organization as it grows.

From an adversarial mindset or systems thinking approach, the recommended resources are necessary to optimize the effectiveness of the network protection approach. An adversarial mindset recognizes that the network protection technology is not foolproof and that attackers may still find ways to bypass the security measures. Therefore, having a dedicated security team or specialist, trained workforce, clear policies and procedures, and appropriate hardware can help detect and respond to security incidents in a timely and effective manner.