Security Policy for an Information System

Darren Pritchard

Department of Cybersecurity, Old Dominion University

CYSE 300

Dr. Joseph Kovacic

January 28, 2023

Designing a security policy for a corporate information system that holds such important and sensitive data is a critical task that requires a thorough understanding of the potential threats and vulnerabilities that the system may face. Points that should be discussed in a security policy for information systems that I will present is not meant to be extensive, nor should it be considered finite. However, that being said, there are five key points to consider in making such a security policy.

Access control is one such crucial aspect of the security policy for a corporate information system. It is important to ensure that only authorized individuals have access to sensitive data stored on the database servers. This can be achieved through the use of strong authentication and authorization mechanisms such as multi-factor authentication and role-based access control. Multi-factor authentication involves requiring multiple forms of identification, such as a password and a fingerprint, to access the system. Role-based access control assigns different levels of access to different users based on their roles within the organization. By implementing these mechanisms, organizations can ensure that only authorized individuals can access sensitive data and protect it from unauthorized access.

The next point to cover is data encryption. Encrypting sensitive data stored on database servers is a crucial step in protecting it from unauthorized access. This includes not only data that's stored on physical devices like hard drives or SSDs, but also data that's transmitted over a network. Encryption ensures that even if someone intercepts the data, they won't be able to read it. There are a variety of encryption techniques available, such as symmetric encryption, asymmetric encryption, and Hashing. To ensure maximum protection, it's vital to use encryption methods that are widely accepted and trusted in the industry.

Another topic to cover in a security policy is network security. Securing a network is crucial to protect against external threats. This involves taking measures such as implementing firewalls to act as a barrier between internal and external networks, keeping an eye out for any suspicious activity with intrusion detection and prevention systems, and breaking up the network into smaller segments to limit the spread of any security breaches and contain them. By taking these steps, organizations can safeguard the perimeter of their network and prevent unauthorized access, data breaches, and other cyber attacks.

Incident response is another critical issue that should be addressed in the security policy for a corporate information system. This includes having a plan in place for how to respond to security incidents, such as data breaches or system failures. The incident response plan should include procedures for identifying, containing, and mitigating the incident, as well as procedures for reporting the incident to the appropriate authorities. It is important to have a designated incident response team responsible for managing the incident, and also to have regular testing and exercises to ensure that the incident response plan is effective and the team is prepared to handle an incident. By having a proper incident response plan in place, organizations can minimize the impact of a security incident, and ensure that they are able to quickly and effectively respond to any incident that occurs.

Compliance with relevant laws and regulations is an important issue to address in the security policy for a corporate information system. This includes ensuring that the information system meets the requirements of regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with these regulations can be achieved through implementing proper security controls such as data

encryption, access control and incident response plans. These regulations may also mandate certain reporting requirements and penalties for non-compliance. It's important for organizations to stay informed about the latest regulations and laws and to adapt their security policies accordingly. By being compliant with relevant laws and regulations, organizations can avoid legal issues and fines, and also demonstrate their commitment to protecting sensitive data and information.

In conclusion, designing a security policy for a corporate information system is a critical task that requires a thorough understanding of the potential threats and vulnerabilities that the system may face. The five important issues that should be addressed in the security policy are access control, data encryption, network security, incident response, and compliance. By addressing these issues, organizations can protect sensitive data stored on their database servers and ensure the security of their information systems.

References

LiquidWeb. (n.d.). *What is an information security policy and how to create one*. Liquid Web. Retrieved January 26, 2023, from https://www.liquidweb.com/blog/information-security-policy/

How to create an information security plan. Agio. (2022, September 26). Retrieved January 26, 2023, from https://agio.com/how-to-create-an-information-security-plan/