Cybersecurity: Security Policy

Raneem Alarian

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 24, 2024

Cybersecurity: Security Policy

Developing a well-written security policy cannot be overstated, especially in today's dynamic and highly digitized world. A well-written security policy serves as a foundational framework, establishing guidelines, procedures, and best practices to protect organizations against potential risks. Five important issues that should be addressed in the security policy for a corporate information system consisting of on-premises web, application, and database servers are access control and authentication, monitoring and logging, incident response, data backup and recovery, and employee training and awareness.

Access Control and Authentication:

A key aspect of any security framework is the establishment of an Access Control and Authentication Policy. Access control defines clear guidelines for who has access to what. In other words, it controls user access to networks, systems, and data (Harvey, 2020). Under this policy, authentication methods such as multi-factor authentication, can help strengthen the verification process and protect data and systems from unauthorized individuals– an important issue that should be addressed in a security policy. This policy is particularly critical for organizations handling sensitive data (Harvey, 2020). Thus, incorporating this in the security policy for a corporate information system that stores sensitive data is essential.

Monitoring and Logging:

A proactive approach to security involves continuous monitoring and logging of system activities. A Monitoring and Logging Policy outlines the implementation of procedures and guidelines for monitoring system activities and logging security events (Harvey, 2020). Through real-time monitoring, an organization can detect and respond to suspicious activities promptly. Without appropriate logging and monitoring, an attacker's activities may go undetected, and logs

imperative to investigating such events may not be available ("Information Security: Logging and Monitoring," 2021).

Incident Response:

An Incident Response Policy guides organizations through the steps to be taken when faced with a security breach. This policy outlines team roles and responsibilities, communication protocols, recovery processes, and planned responses (Harvey, 2020). A well-designed incident response plan can help minimize the impact of security incidents, facilitate a swift response, and secure the overall organization. This policy not only reduces the response time of a security incident but also the overall cost associated with it (Price, 2023).

Data Backup and Recovery:

The Data Backup and Recovery Policy outlines strategies for regular backups, storage procedures, and recovery processes. Organizations handling sensitive information must implement this policy to ensure business continuity in the face of cyber incidents, system failures, or natural disasters (Harvey, 2020). Therefore, implementing this in a security policy can address the issue of data loss and mitigate the impact of a cyberattack.

Employee Training and Awareness:

Employee Training and Awareness addresses security risks and vulnerabilities by fostering a culture of security consciousness among employees and staff members. Regular training programs educate employees on security best practices, the importance of protecting sensitive data, and how to identify potential security threats. According to the Center for Internet Security, cybersecurity awareness training for employees helps minimize risks that come from the human element (2023). Implementing this in organizations and businesses is a critical part of fostering an informed and safer workforce.

References:

Harvey, S. (2023). 15 information security policies every business should have. *KirkpatrickPrice*. https://kirkpatrickprice.com/blog/15-must-have-information-security-policies/

Information security: Logging and monitoring. (2022). UW Policies. https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-logging-and-monitoring/#:~:text=Ensuring%20system%20logs%20are%20available,the%20potential%20impact%20of%20incidents.

Price, J. (2023). 5 benefits of an incident response plan. *SubRosa.* https://subrosacyber.com/blog/5-benefits-of-an-incident-response-plan#:~:text=An%20incident%20response%20plan%20helps,its%20impact%20on%20other%20operations.

Why employee cybersecurity awareness training is important. (2022). CIS. https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important