6-1 Project One: Network Evaluation Report

Joshua Merren

Southern New Hampshire University

CYB-310-13414-M01 Network Defense

Professor Megan Buckner

9 October 2024

The lack of comprehensive password policy best practices in an organization often stems from a need for more awareness about cybersecurity risks and the harmful impact of weak password policies on network security. This negligence can be attributed to insufficient training programs and a lack of dedicated cybersecurity leadership. This leaves organizations vulnerable to attacks such as brute force and credential stuffing, where commonly used or outdated passwords are exploited. Organizations need enforceable standards and regular updates to password management protocols to avoid exposing themselves to miscellaneous threats. Furthermore, failing to establish and maintain strict password policies can lead to non-compliance with industry regulations and standards, which can have legal and financial repercussions aside from the obvious security implications.

To rectify this, adopting a password management strategy that incorporates NIST's best practices is essential. These practices, which recommend passwords of at least 12 characters incorporating a mix of uppercase, lowercase, numeric, and special characters, are widely recognized for their effectiveness. Regular updates to password policies should include measures to avoid using previously breached passwords and enforce password changes at defined intervals. Using password enhancement techniques like hashing and salting, alongside implementing account lockout mechanisms after several failed login attempts, will strengthen security. Additionally, educating employees on the importance of strong, unique passwords and the potential risks of poor password hygiene is critical. The inclusion of technical measures and employee education will together reinforce the security framework within the organization (Grassi et al., 2017).

A strict password policy significantly reduces the risk of unauthorized access, protecting the organization's data integrity and confidentiality. By encouraging tough passwords and understanding the need for regular updates, employees become more security-aware, contributing to a robust organizational security culture. These steps ensure compliance with data protection regulations and mitigate potential legal and financial repercussions. Furthermore, adopting recommendations from security experts like Poza (2020), who emphasize the evolution of password guidelines to enhance security protocols, supports the continual improvement of security measures within the organization. This proactive approach secures the network and aligns with industry-leading practices, promoting a culture of security and caution beyond mere compliance.

Interdepartmental access issues often stem from inadequate access controls and an insufficient understanding of the principle of least privilege. These issues usually stem from the initial setup of access permissions or failures to update permissions as employee roles and departmental functions evolve. As organizations grow, they may need to scale their access control policies sufficiently, which often results in permissions needing to be narrower and more aligned with individual job requirements. This misalignment can lead to scenarios where employees can access more systems and data than necessary, increasing the risk of accidental and deliberate data breaches. With a dynamic approach to managing access permissions, organizations can avoid security lapses that seriously affect data integrity and regulatory compliance.

To address these challenges, the organization should adopt a robust role-based access control (RBAC) system, which assigns network permissions based on individual employees' specific roles and responsibilities. This system must be dynamic to allow for easy updates to access rights as employee roles change or as the organizational structure evolves. Implementing RBAC requires defining clear roles and access permissions, conducting regular audits, and ensuring that these roles and permissions accurately reflect the current organizational needs. RBAC helps simplify access management by grouping users based on roles, simplifying the permissions each group receives, enhancing security, and reducing the potential for errors. Furthermore, integrating additional security measures such as comprehensive logging and monitoring of access requests and employing multi-factor authentication can significantly enhance system security against unauthorized access (LastPass, 2024; Hussey, 2022).

Implementing a strict RBAC system significantly enhances organizational security by ensuring that employees have access only to the data and systems necessary for their roles. This minimizes unnecessary access to sensitive information, thereby reducing the risk of security breaches. Regular audits and reviews of access permissions are crucial for maintaining the integrity of the access control system and ensuring it remains aligned with organizational changes. Adhering to RBAC's best practices secures the organization's data and systems and ensures compliance with regulatory requirements, protecting the organization's reputation and legal standing. This proactive approach to access management supports a secure, efficient, and compliant operational environment, demonstrating a commitment to security and compliance that is critical for modern businesses (McCarthy, 2024).

References

Grassi, P. A., Garcia, M. E., Fenton, J. L., Applied Cybersecurity Division, Information Technology Laboratory, Altmode Networks, U.S. Department of Commerce, National Institute of Standards and Technology, Jr. Ross, W. L., & Rochford, K. (2017). NIST Special Publication 800-63-3 Digital Identity Guidelines. In *NIST Special Publication 800-63-3* [Report]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Hussey, K. (2022, June 23). *Role-based access control best practices*. TDi. Retrieved October 9, 2024, from https://www.tditechnologies.com/2022/06/22/role-based-access-control-best-practices/

LastPass. (2024, August 30). *Role-Based access control explained | LastPass - The LastPass blog*. Retrieved October 9, 2024, from https://blog.lastpass.com/posts/2024/08/role-based-access-control

McCarthy, M. (2024, April 8). *The Definitive Guide to Role-Based Access Control (RBAC) | StrongDM*. Retrieved October 9, 2024, from https://www.strongdm.com/rbac

Poza, D. (2020, January 22). *diagram_desktop* [Video]. Auth0 - Blog. Retrieved October 9, 2024, from https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/