Joshua Farias

Professor Cooper

SEC 605

24th March 2024

Best Practices for User Domain Compliance

1) Strong Password Policies & Multi-Factor Authentication (MFA)

Enforce the use of complex passwords and require MFA to add an extra layer of security. Complex passwords should contain a mix of alphanumeric characters, symbols and should not be based on dictionary words.

Reference: *National Institute of Standards and Technology (NIST), Special Publication 800-63-3, Digital Identity Guidelines.*
*(**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf**)*

2) User Awareness Training & Acceptable Use Policies

Training should be conducted periodically to educate staff on cybersecurity risks, phishing awareness and safe computing practices. This ensures that users within the company understand their roles in the company in maintaining security.

Reference: *National Institute of Standards and Technology (NIST), Special Publication 800-63-3, Digital Identity Guidelines.*
*(**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf**)*

3) Regularly Update Security Patches

Apply necessary patches for software to fix known vulnerabilities and mitigate potential security risks.

Reference: *Rapid7, Patch Management Definition & Best Practices*

*(**https://www.rapid7.com/fundamentals/patch-management/**)*

4) Role Based Access Control (RBAC)

It is a good security practice to follow the principle of least privilege and this can be achieved through role based access control. Role based access control ensures that users within an organization only have access to resources they need to complete their daily work tasks. This minimizes the risk of unauthorized access to sensitive information.

Reference: *Red Hat Inc. What is Role Based Access Control (RBAC)?*

*(**https://www.redhat.com/en/topics/security/what-is-role-based-access-control**)*

5) User Monitoring

Implement monitoring software and IDPS systems to detect and respond to suspicious behavior promptly.

Reference: *National Institute of Standards and Technology (NIST), Special Publication 800-92, Guide to Computer Security Log Management*

(https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf)

6) Secure Workstations for Elevated Accounts

Use clean OS install, apply hardening security baselines, enable full disk encryption, restrict access to USB ports and use VMs for safer administrative tasks to mitigate risks associated with local threat actors.

Reference: *Active Directory Pro, Top 25 Active Directory Best Security Practices*

(https://activedirectorypro.com/active-directory-security-best-practices/)

7) Secure Remote Access

Ensure authorized users can remotely access the network with secure methods. Implement authentication and encrypt sessions using VPNs to safeguard against unauthorized access and enhance confidentiality and integrity.

Reference: *National Institute of Standards and Technology. (2020). SP 800-53 Rev. 5*

(https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) pg. 48

8) Implement Account Lockout Policies

Further more software such as IDS software can be implemented to stop threat actors from brute forcing email accounts. The software can be configured to temporarily or permanently block login requests from suspected threat actors after they get so many passwords incorrect, furthermore IDS have logging features that contain the suspected threat actors IP address and the credentials they attempted to login as, which can be analyzed for further threat intelligence.

Reference: *NIST Special Publication 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management.*

(https://pages.nist.gov/800-63-3/sp800-63b.html)

9) Regularly Review User Accounts

Periodic reviews of user accounts should be conducted to identify and deactivate dormant accounts, ensuring that only active and authorized accounts remain in the system.

Reference: *ISACA, Effective User Access Reviews*

(https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews)

10) Encrypt Sensitive Data

Encryption techniques should be utilized to protect sensitive data both at rest and in transit, safeguard it from unauthorized access or interception.

Reference: *Precisely, Data Encryption Best Practices*

(https://www.precisely.com/blog/data-security/data-encryption-101-guide-best-practices)

11) Establish Data Retention and Deletion Policies

Define clear policies for data retention and deletion that comply with legal requirements and ensure unnecessary data is securely disposed of.

Reference: *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*

*(**https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917935**)*

12) Regular Security Assessments

Security assessments, including vulnerability assessments and penetration testing should be conducted regularly to identify and remediate potential security weaknesses proactively.

Reference: *Open Web Application Security Project (OWASP), OWASP Testing Guide.*

*(**https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf**)*