Strong Password Policies Assignment

Student: Tania Diaz
Course: CIST-2881-D1
Module: 1

Introduction

Passwords are one of the first lines of defense against cyber threats. A strong password policy ensures that users create passwords that are difficult to guess, protecting both personal and organizational data. Organizations enforce these policies to maintain consistency and reduce the risk of hacks, scams, or unauthorized access. Strong password policies not only protect the organization but also educate users on security best practices.

Top Ten Password Policies I Would Deploy

- ★ **Minimum Password Length**
    - **Policy:** Require passwords to have at least 12 characters.
    - **Reason:** Longer passwords are harder for attackers to crack using brute-force attacks (NIST, 2017).
- ★ **Password Variety Requirement**
    - **Policy:** Passwords must include uppercase, lowercase, numbers, and symbols.
    - **Reason:** Adding variety strengthens passwords against dictionary or guessing attacks.
- ★ **Mandatory Password Changes**
    - **Policy:** Users must update passwords every 90 days.
    - **Reason:** Limits the damage if a password is compromised (CIS, 2021).
- ★ **Ban on Common Passwords**
    - **Policy:** Prevent users from using weak or easily guessed passwords such as “123456” or “password.”
    - **Reason:** Simple passwords are frequently targeted and easy for attackers to guess.
- ★ **No Password Reuse**
    - **Policy:** Users cannot reuse any of their last 5 passwords.
    - **Reason:** Encourages the creation of new, unique passwords over time.
- ★ **Two-Step Verification (MFA)**
    - **Policy:** Require multi-factor authentication for all logins.
    - **Reason:** Provides an extra layer of protection even if a password is stolen (NIST, 2017).
- ★ **Account Lockout After Failed Attempts**

- **Policy:** Temporarily lock accounts after 5 failed login attempts.
- **Reason:** Prevents repeated attempts from brute-force attacks.

★ **Encrypted Password Storage**

- **Policy:** Store passwords using strong encryption and salted hashes.
- **Reason:** Protects passwords in case of a system breach (OWASP, 2020).

★ **Secure Password Recovery**

- **Policy:** Password reset requests must include verification through email or phone.
- **Reason:** Prevents unauthorized users from gaining access through resets.

★ **User Training on Password Security**

- **Policy:** Provide education on creating strong passwords, avoiding password reuse, and recognizing phishing attempts.
- **Reason:** Informed users are less likely to make mistakes that compromise security (CIS, 2021).

Conclusion

A strong password policy combines technical rules with user education to protect sensitive data and prevent unauthorized access. These policies help create a secure environment without relying solely on individual user behavior. By using a combination of complexity, enforcement, and awareness, organizations can significantly reduce the risk of security breaches.

References

Center for Internet Security. (2021, May 18). *CIS Critical Security Controls version 8* [Press release].https://www.cisecurity.org/controls

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A., & Burr, W. E. (2017, June). *NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management* (SP 800-63B Rev. 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b

Manico, J., Saad, E., Maćkowski, J., & Bailey, R. (2020, April). *OWASP Password Storage Cheat Sheet*. Open Worldwide Application Security Project. https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html?