PASSWORD POLICY IN A ORGANIZATION

Implementing a robust password policy is crucial for maintaining security within an organization

❑Require passwords to be complex, including a mix of upper and lower case letters, numbers, and special characters. Use random characters.This helps from basic dictionary attacks and enhances overall security

❑Set a minimum password length, typically at least 8 characters. Longer passwords are generally more secure.

❑A complex password is one that incorporates a diverse range of characters making it more difficult for attackers to guess or crack using automated tools.

Some common components of password complexity that help to secure passwords

Uppercase Letters: Including uppercase letters (A-Z)
Lowercase Letters: including lowercase letters (a-z) increase compexity of password

Numbers (Digits): Adding numbers (0-9) to the password increases its randomness and makes it harder to guess.

Special Characters: Special characters (!, @, #, $, %, etc.) further enhance password complexity. They add a wider range of characters that an attacker would need to guess, significantly increasing the time and effort required to crack the password.

Minimum Length: Setting a minimum length for passwords ensures that they are not too short and provides more space for incorporating complex character combinations. Common minimum lengths range from 8 to 12 characters, although longer passwords are generally considered more secure.

Avoiding Dictionary Words: Passwords should avoid using common dictionary words or easily guessable combinations as these can be susceptible to dictionary attacks.

Common password problems

Often involves implementing robust security measures, educating users on best practices and providing support and guidance when needed. This can help mitigate security risks and ensure a smoother user experience when it comes to managing passwords.Common problems include:

- Forgetting Passwords
- Password Reuse
- Weak Passwords
- Expired Passwords
- Too many sites/passwords to manage

Common password threats that individuals and organizations face include

Brute Force Attacks: Attackers use automated tools to systematically try different combinations of characters until they find the correct password. This is more likely to succeed with weak or easily guessable passwords.

Dictionary Attacks: dictionary attacks involve trying commonly used words, phrases, and combinations found in dictionaries and password lists. This method is effective against weak passwords.

Password Guessing: Attackers guess passwords based on information they know about the user, such as personal details, interests, or commonly used patterns.

Insider Threats: Employees or individuals with authorized access may misuse their privileges to steal passwords or access sensitive information for malicious purposes.

PASSWORD MANAGERS

Password managers are tools designed to securely store and manage passwords for various online accounts and services. They offer several benefits

- A software That stores your passwords
- Can generate Random and complex Passwords
- Syncs your passwords and makes them available on the device you use even without internet access
- Example
  - 1Password
  - Lastpass
  - Nordpass

Organizations should consider alternative security measures and best practices such as

- Strong password policies
- Multi-factor authentication
- User education
- In conjunction with or in place of password expiry

maintain strong security posture while minimizing user inconvenience.