Password Policies

WHAT ARE PASSWORD POLICIES?

REQUIREMENTS OF PASSWORD POLICIES

The Problems Surrounding Passwords

- This increase in password use is largely due to the increase of online services (Social Media), including those provided by government and the wider public sector.
- Passwords are an easy to implement and a low-cost security measure.
- However, this increase of the use of passwords, and the growing need to use a complex password systems, it can place impracticable requirements on users.

The Problems Surrounding Passwords

- Generally users will develop their own methods to deal with ‘password overload’.
- Some methods users may employ include, writing down passwords, re-using the same password across different systems, or using simple and predictable password.
- A study within a Scottish NHS trust found that 63% of its users admitted to re-using passwords.

Password Policies

What is a Password Policy?

A password policy is a set of rules used to enhance computer security by encouraging users to employ a strong password structure and use them correctly.

A password policy is regularly used by organization's to meet the requirements of official regulations/legislations and will more than likely be taught as part of the organisations security awareness training.

Password policy can sometimes only be a advisory process, but usually, the computer system will force users to comply with the in place password policy.

Password Policies

What is included in Password Policies?
Password Policies will generally focus on the following areas

- **Password length and formation**
- **Password blacklists**
- **Password duration**
- **Usability considerations**

Password length and formation

- Most password policies will require a minimum password length.
- Eight characters is generally the minimum required length, but some organisations may choose to increase this to enhance security .
- Longer passwords are generally thought of as being more more secure, but some systems impose a maximum length for compatibility with older legacy systems.

Password length and formation

- Some policies will impose conditions on the user to what type of password they can create, such as:
- Use of both upper-case and lower-case letters (case sensitivity)
- The use of one or more numerical digits
- The use of special characters, such as @, #, $
- The exclusion of words found in a password blacklist
- The exclusion of words found in the user's personal information
- The exclusion of use of company name or an abbreviation
- The exclusion of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers
- Other systems may pre populate password for the users or allow the user to select one from a list of displayed choices.

Password blacklists

- Password blacklists can be described as lists of passwords that are always blocked from use by users.
- Blacklists contain passwords constructed of character combinations that meet a organisations password policy, but should no longer be used because they have been deemed insecure for one or more reasons
- Reason could be, passwords that can be easily guessed, passwords that follow a common pattern, or passwords that have been publicly disclosure due to a previous data breaches.
- Common examples are Password1, Qwerty123, or Qaz123wsx.

Password duration

- Most Password policies force users to change passwords on a regular basis, it can range every 90 or 180 days, depending on the policy.
- The advantages of changing passwords on a regular basis, is questionable. Systems that implement these policies can prevent users from choosing a password that is to similar to a previous selection.
- Users can find it difficult to create passwords that are also easy to remember.
- If it a necessity for users to change their passwords regularly, this can also result in users creating much weaker passwords, due to the fact the change there password so often.

Usability considerations

- Password policies are a trade-off between theoretical security and the practicalities of human behaviour.
- Using extremely complex passwords and forcing the user to change passwords frequently can lead users to write passwords down on post-it note near there computer.
- Users will generally have a number of passwords to remember, & making sure users never write down their passwords may be impractical for the user and also lead to the creation of weak passwords.

Password Policy Tips

- Change all default passwords
- Help users cope with password overload
- Understand the limitations of user-generated passwords
- Understand the limitations of machine-generated passwords
- Prioritise administrator and remote user accounts
- Use account lockout and protective monitoring
- Don’t store passwords as plain text