SPECOPS

The IT Director's guide to passwords and Cyber Essentials

This guide details how password policy and password security play a role in achieving Cyber Essentials accreditation.

Cyberattacks are on the rise in the UK. The number of cyberattacks made on UK businesses in the first quarter of 2019 increased 122 percent compared to last year. The Cyber Essentials scheme is a UK government certification that provides guidance to help organisations guard against common cyberattacks. According to the UK government, the Cyber Essentials security controls can prevent around 80% of cyberattacks. The controls are mandatory for all government contracts that involve handling personal information, and delivering certain information communications technology products.

There are five technical control topics included in the scheme:

- Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Patch Management

When it comes to password security, the Cyber Essentials scheme offers clear guidelines. After all, password exploitation remains the leading cause of many data breaches. Password-specific requirements can be found in the Secure Configuration and User Access Control sections of the Cyber Essential Scheme.

ABOUT SPECOPS

Specops Software develops unique password management and desktop management products based on Microsoft technology. We build on top of Active Directory and Group Policy with innovative, simple, and cost-efficient solutions for organizations around the world.

specopssoft.com/blog

Secure Configuration and passwords

The objective of Secure Configuration is to ensure that computers and network devices are configured to reduce the level of inherent vulnerabilities. Devices should only provide the service required to fulfil their role. In addition to computer and network device requirements, Secure Configuration details password-based authentication. In a shift away from password complexity, the requirements place the technical password burden on systems, as opposed to relying on users following good practices. To achieve the certificate an applicant must fulfil the following (from the Cyber Essentials website):

Protect against brute-force password guessing, by using at least one of the following methods:

- lock accounts after no more than 10 unsuccessful attempts
- limit the number of guesses allowed in a specified time period to no more than 10 guesses within 5 minutes

Set a minimum password length of at least 8 characters.

Not set a maximum password length.

Change passwords promptly when the Applicant knows or suspects they have been compromised

Have a password policy that tells users:

- how to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet)
- not to choose common passwords — this could be implemented by technical means, using a password blacklist
- not to use the same password anywhere else, at work or at home
- where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
- if they may use password management software — if so, which software and how
- which passwords they really must memorize and not record anywhere

The Applicant is not required to:

- enforce regular password expiry for any account (we actually advise against this — for more information see The problems with forcing regular password expiry)
- enforce password complexity requirements

Access Control and passwords

User Access Control ensures user accounts are assigned to authorized individuals only. Access should only be granted to those applications, computers, and networks that are actually required for the user to perform their role. You can reduce the risk of information being stolen or damaged by granting only as much access as needed. This technical control defines requirements of privileged accounts and processes for limiting access. The requirements include the following (from the Cyber Essentials website):

- have a user account creation and approval process
- authenticate users before granting access to applications or devices, using unique credentials (see Password-based authentication)
- remove or disable user accounts when no longer required (when a user leaves the organization or after a defined period of account inactivity, for example)
- implement two-factor authentication, where available
- use administrative accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)
- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Account lockouts to defend against brute-force attacks

In a brute-force attack, a bot attempts every password combination of words and numbers until they find the password that gives them access to the network. When used against short and simple passwords, the attack is often successful. In recent years, high profile victims have brought these attacks to the forefront. In 2017, Westminster Parliament fell victims to a brute force attack, resulting in the compromise of 90 email accounts. In 2018, the accounts of several members of the Northern Irish Parliament were accessed by brute-force attackers.

To protect your organisation against brute-force attacks, the Cyber Essentials scheme recommends account lockouts – locking accounts after 10 failed login attempts. Since many brute-force attacks likely happen in a short period, the Cyber Essentials scheme further suggests to limit the number of guesses to no more than 10 guesses within 5 minutes. There are times when unsuccessful login

Use a password blacklist

The Cyber Essentials scheme urges organisations to concentrate efforts on technical controls to steer users away from picking common and compromised passwords, such as using a password blacklist. A password blacklist is a list of disallowed passwords consisting of common and compromised passwords. It improves security as it prevents hackers from exploiting weak passwords.

A blacklist can be created from published lists of common passwords. The NCSC offers a list of 100,000 of the most common passwords, which is just the tip of the iceberg when it comes to passwords. With tens of billions of leaked passwords available online, using a comprehensive blacklist is critical. Additionally, to stay protected against new threats, organisations will need to continually grow and update their list. A third-party password blacklisting service can simplify the process of managing the list of leaked passwords.

Expire passwords only when necessary

The NCSC and Cyber Essentials scheme both recommend a password change only when a compromise is known or suspected. Even though periodic changes can prevent indefinite access via compromised credentials, they can have a negative effect on both security and usability. Already dealing with password overload, users are likely to fall into predictable patterns when choosing a new password or resort to writing down their passwords.

Before stopping periodic password changes, you'll need another system defence in place. Whether it is a monitoring tool to detect compromised passwords, multi-factor authentication, you need a way to detect and prevent unauthorized access. Length-based password aging should be considered as it rewards users for choosing longer passwords by extending the expiration period.

Password preparation for Cyber Essentials

If you are planning for Cyber Essentials accreditation you will need to make sure your password policy is up to the challenge. Shift the password burden away from your users, and place it instead on the technical systems. For example, you could use a password blacklist to stop leaked passwords, lock accounts after repeated login attempts, and stop periodic password expirations while continually checking for compromised passwords. You should also limit the number of users who have privilege access, and use those accounts for only the task that is required of them.