Courtesy of ABEX

CYBERRISKS&LIABILITIES_

Managing Password Threats

Organizations trust passwords to protect valuable assets such as data, systems and networks. Passwords are versatile—they authenticate users of operating systems (OS) and applications such as email, labour recording and remote access, and they guard sensitive information like compressed files, cryptographic keys and encrypted hard drives.

Because passwords protect such valuable data, they are often a prime target of hackers and thieves. Although no method of password protection is 100 per cent effective, it is still important to understand and mitigate threats to password security so you can protect your company and its assets.

Types of Password Threats

Implementing security measures starts with anticipating security threats. There are four main ways that attackers attempt to obtain passwords: capturing passwords, guessing or cracking passwords, replacing passwords and using compromised passwords.

1. **Password Capturing**

   An attacker can capture a password through password storage, password transmission or user knowledge and behaviour. OS and application passwords are stored on network hosts (a computer connected to a network) and used for identification. If the stored passwords are not secured properly, attackers with physical access to a network host may be able to gain access to the passwords. Never store passwords without additional controls to protect them. Security controls include:

   - Encrypting files that contain passwords
   - Restricting access to files that contain passwords using OS access control features
   - Storing one-way cryptographic hashes for passwords instead of storing the passwords themselves

   Hashes are the end result of putting data, like passwords, through an algorithm that changes the form of the original information into something different. For example, the password ‘default’ could be mapped as an integer such as 15. Only the network host knows that 15 stands for the password ‘default’.

   Using hashes allows computers to authenticate a user’s password without storing the actual password. However, organizations should assess which applications are allowed to store passwords or hashes based on the risks, rather than on convenience for the user. This assessment should be reflected in the organization’s password policy.

   Even when passwords are protected with hashes, an attacker can still uncover them via transmission. When a user enters a password into a computer, the password or hash is often transmitted between hosts over the network to authenticate that user. This transmission action is vulnerable to attack. You can reduce this risk by encrypting your passwords or the transmissions containing the passwords.

   Organizations can also avoid transmission risks by storing passwords on paper. Such papers should be physically secured in a locked safe or file cabinet. Be sure to properly discard any password-containing papers by shredding them.

   However, storing passwords on paper cannot protect against means of capturing passwords that rely on user behaviour such as malware. For example, Trojan horses and keylogger malware observe user activity, such as which keys a user presses, to discover his or her username and passwords. Mitigate these threats by regularly scanning your computers with antimalware and antivirus software.

Users can also endanger password security by responding to phishing attempts, which relocate a user to a malicious website posing as a legitimate one that asks for sensitive information such as usernames and passwords. Caution your employees against downloading files from unknown sources.

2. **Password Guessing and Cracking**
   Attackers attempt to discover weak passwords through guessing, and recover passwords from password hashes through cracking.

   Guessing is simple: An attacker attempts to uncover a password by repeatedly guessing default passwords, dictionary words and other possible passwords. Anyone who has access to the authentication interface can try to guess a password. That is why strong passwords are necessary for cyber security. Never pick a password that someone could easily guess, and make sure to reasonably limit the number of authentication attempts to prevent unlimited guessing.

   Cracking is a little more complicated. Attackers gain access to password hashes and attempt to discover a character string that will produce the same encrypted hash as the password. If the hash algorithm is weak, cracking is much easier. Hash functions should be one-way, meaning passwords only go from original to encrypted, not vice versa. Hash functions make it nearly impossible to derive the original text from the character string. As with guessing, cracking can also be prevented by choosing strong passwords and periodically changing them.

3. **Password Replacing**
   When users forget their passwords, they have two options: reset the password (change it to a new one) or recover the password (get access to the current one). If the user's identity is not properly verified in a reset or recovery request, an attacker could easily pose as the user, gain unauthorised access to the system, application or data and provide a password that only he or she knows. This replaces the user's original password with something unknown, barring the user from the system.

   All attempts to reset or recover a password should start with a rigorous verification process. Verification should not hinge on information that can be easily obtained, such as birth date, employee number or mother's maiden name. Instead, consider personal or subjective information that only the user knows.

4. **Compromised Passwords**
   When an attacker compromises a password through any of the previously mentioned methods, that attacker will have unauthorized access until the user changes his or her password. For this reason, many organizations use automatic password expiration measures to ensure no password remains valid forever.

   Yet password expiration is futile if the root cause of a compromised password is not fixed. For example, if an attacker uses cracking to obtain a password, automatic password expiration will not solve the security problem because the attacker can simply use the same process again. If you use automatic password expiration, make sure you have a plan in place to secure your system and reset passwords in the event of a security breach. When one password is compromised, reset all passwords just to be safe.

Password Management
On-going password management will help prevent unauthorized attackers from compromising your organisation's password-protected information. Effective password management protects the integrity, availability and confidentiality of an organization's passwords.

Integrity and availability should be ensured by typical data security controls, such as using access control lists to prevent attackers from overwriting passwords and having secured backups of password files. Confidentiality, on the other hand, is much harder to ensure—it involves implementing diverse security measures and making decisions about the nature of passwords themselves. For example, organizations should encourage users to choose long, complex passwords with a mixture of numbers and letters. However, complex passwords are harder to remember, which means users are more likely to write them down and subsequently endanger the system's security. This presents a dilemma in which one security measure (choosing a long, complex password) conflicts with another (never writing down your password).

Protecting Your Passwords

You can help resolve conflicting security measures by implementing the following security recommendations:

- Create a password policy that specifies all of the organization's password management-related requirements.
- Protect passwords from attacks that capture passwords.
- Configure password mechanisms to reduce the likelihood of successful password guessing and cracking.
- Determine requirements for password expiration based on balancing security needs and usability.

Managing an organization's password security risk can be a difficult process—threats are unrelenting. Contact ABEX for more information on mitigating your cyber risks.