MS-ISAC

MS-ISAC Security Primer

Securing Login Credentials

March 2017, SP2017-0514

Malicious actors regularly release login credentials from compromised databases. Cyber criminals can use these credentials in many ways, including to impersonate individuals online, gain access to work and personal accounts, sign online service agreements or contracts, engage in financial transactions, or change account information

PASSWORD POLICY RECOMMENDATIONS:

- Passwords should have at least ten characters and include uppercase and lowercase letters, numbers, and symbols. CIS recommends the use of 14 characters.
- Use different passwords for each account you access.
- Do not use words and proper names in passwords, regardless of language, or personal information, such as your name, a family member or pet's name, etc.
- Change passwords regularly -- at least every 60 days; if you believe your account has been compromised change passwords immediately. Do not reuse old passwords.
- Do not allow a browser's password manager to store your passwords; some browsers store and display passwords in clear text and do not implement password protection by default.
- Do not allow websites to automatically log in to an account; many services store this information locally and it can be exploited by attackers to gain access without a password.
- Do not share your password with anyone and do not respond to emails or phone calls asking for your login credentials. Legitimate businesses will never ask for your login credentials via these methods.
- At work, follow your organization's password policy and use different passwords for work and personal use. Do not use your work email when joining and accessing personal websites.
- Use multi-factor authentication consisting of something you know (password) and something you have (mobile phone, physical key, etc.), if it is offered.

TECHNICAL RECOMMENDATIONS:

- Implement network controls to enforce your organization's credential policies.
- Maintain a password history sufficient to prevent users from reusing any password used in the last year. CIS recommends preventing users from using any of the last 24 passwords.
- Implement controls that ensure passwords are changed at least every 60 days.
- Set the minimum password age to at least 1 day, so users cannot cycle through passwords to return to their favorite password (e.g. changing a password 24 times in 25 minutes, to allow them to reuse the original password).
- Require that all passwords contain at least three of the following four categories: uppercase and lowercase letters, numbers, and/or symbols.
- Store all passwords using strong salting and hashing functions; only those with super-user privileges should be able to access the stored file. Do not store passwords using reversible encryption.
- Set account logout thresholds to 10 or fewer invalid login attempts, and require at least 15 minutes between an account lockout and password reset. Log and monitor all login attempts.
- Change default passwords and administrator accounts when setting up new equipment.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.