User Management

Some of the most commonly exploited vulnerabilities are those that take place where the user meets the machine. User accounts get hijacked and are used to access resources, sometimes methodically over time, to access valuable resources or cause damage.

To reduce the risk of user account incidents, you need to implement strong protections on every user account and limit the amount of damage that may be caused by takeover of a single user account.

1. Passwords: Like it or not, passwords are a reality of online life and will be for some time to come. They are also a common vector of attack by threat actors. You can't have good user management without good password policies.
2. Multi-factor authentication (MFA): The best way to address weaknesses in authentication is to have the right MFA requirements in place–those that, through a variety of means, use at least two of something you know (like a password), something you have (like a cell phone), and something you are (like a fingerprint) to log in.
3. User accounts: How you manage user accounts–creating, managing, tracking, and deleting–can have a huge impact on your overall cybersecurity posture.

Goals

1. Implement good password practices (Level 1 maturity)
2. Implement MFA wherever possible (Level 1 maturity)
3. Ban or limit shared or generic accounts (Level 1 maturity)
4. Employ least privilege, especially with administrative access, and revoke access appropriately (Level 1 maturity)
5. Log user activity (Level 1 maturity)

Actions

For User Management, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

User Recommendations

1. Do not reuse passwords across multiple platforms, systems, or software. This includes never using the same login credentials for work and personal use.
2. Never create passwords or security questions using personal information, such as your name, children's names, dates of birth, etc., that someone might already know or can easily obtain.
3. Use passphrases, ideally of at least four words of 5+ letters, instead of random sets of characters. If you do this, you don't need to use composition rules like upper, lower, number, and symbols. An example of a good passphrase is "blender saute pendant chair."
4. Enable MFA anywhere it's offered, on all accounts, for all applications. This is especially true for anything accessed outside your environment, including social media accounts, and any access back into your environment from outside. Ensure this is true for all IT products supplied by vendors.
5. Use a password manager, and protect access to it with MFA.

Organizational Recommendations

1. Remove all default accounts or change the default password on all accounts, applications, and systems.
2. Enable MFA anywhere it's offered, on all accounts, for all applications. This is especially true for anything accessed outside your environment, including social media accounts, and any access back into your environment from outside. Ensure this is true for all IT products supplied by vendors.
3. Store all passwords and passphrases using salting and hashing functions and **not** with encryption. Make sure your vendors do the same.
4. Set login thresholds to 10 or fewer invalid login attempts before locking the user out and increase the interval between a failed attempt and allowing the next attempt. Log and monitor all login attempts.
5. Ban or limit shared or generic accounts.
   - Realistically, some devices or applications may require shared accounts. These accounts should receive formal exceptions from management and their usage appropriately tracked.
   - When this is the case, rotate passwords, passcodes, and biometrics (like TouchID) when reasonable, like with each election.
6. Employ least privilege by only giving a user access to the devices, applications, and services they need to do their jobs. This limits the damage that may be caused by takeover of any single account. This is particularly important for any account with administrative access to sensitive network controls or confidential materials.
7. Review individuals' access and revoke any unnecessary or inappropriate access. Establish a plan to do this regularly, and make it part of the offboarding and job change processes to ensure that user has access to what they need and nothing else.
8. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.
9. Employ user logging on your networks. You should be able to see whenever a user logs into a device or network. Maintain records of these logs.
10. Allow and encourage use of password managers.

Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Complete all of the actions for the Level 1 maturity.
2. Review MS-ISAC's Security Primers on Exposed Credentials and Securing Login Credentials, as well as the United States Computer Emergency Readiness Team's (US-CERT's) Security Tip on Choosing and Protecting Passwords.
3. The EI-ISAC regularly monitors the Internet for stolen credentials using open source datasets from various security organizations and researchers, as well as information received from trusted partners. To subscribe to this service, simply provide your IP addresses and domains to soc@cisecurity.org.
4. Use services to search for breaches of your users' email addresses and passwords.

Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Beyond Simple Passwords: A toolbox with links to free tools relevant to this best practice.
- have i been pwned password breach service: A site for searching for breached accounts. Includes and API to automate searching for breached accounts.

Learn More

- Get more password guidance from NIST: SP 800-63B Section 5.1.1.2.
- Password spotlight (This spotlight has some out-of-date recommendations. Use in conjunction with the NIST guidance).
- Understand the logic behind using passphrases.

Mapping to CIS Controls and Safeguards

- 3.3 Configure Data Access Control Lists (Level 1 maturity)
- 4.7: Manage Default Accounts on Enterprise Assets and Software (Level 1 maturity)
- 5.1: Establish and Maintain an Inventory of Accounts (Level 1 maturity)
- 5.2: Use Unique Passwords (Level 1 maturity)
- 5.3: Disable Dormant Accounts (Level 1 maturity)
- 5.5: Establish and Maintain an Inventory of Service Accounts (Level 2 maturity)
- 5.6: Centralize Account Management (Level 2 maturity)
- 6.1: Establish an Access Granting Process (Level 1 maturity)
- 6.2: Establish an Access Revoking Process (Level 1 maturity)
- 6.3: Require MFA for Externally-Exposed Applications (Level 1 maturity)
- 6.4: Require MFA for Remote Network Access (Level 1 maturity)
- 6.5: Require MFA for Administrative Access (Level 1 maturity)
- 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems (Level 2 maturity)
- 6.7: Centralize Access Control (Level 2 maturity)
- 6.8: Define and Maintain Role-Based Access Control (Level 2 maturity)
- 3.14 Log Sensitive Data Access (Level 3 maturity)

Mapping to CIS Handbook Best Practices

- 24, 25, 26, 47, 49, 50, 51, 52, 66, 77, 78, 81