CONTROL 5

Account Management

Safeguards: 6	IG1: 4/6	IG2: 6/6	IG3: 6/6

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why is this Control critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in CIS Control 8 (Audit Log Management), it is important in the development of a comprehensive Identity and Access Management (IAM) program.

Procedures and tools

Accounts must be tracked; any account that is dormant must be disabled and eventually removed from the system. There should be periodic audits to ensure all active accounts are traced back to authorized users of the enterprise asset. Look for new accounts added since previous review, especially administrator and service accounts. Close attention should be made to identify and track administrative, or high-privileged accounts and service accounts.

Users with administrator or other privileged access should have separate accounts for those higher authority tasks. These accounts would only be used when performing those tasks or accessing especially sensitive data, to reduce risk in case their normal user account is compromised. For users with multiple accounts, their base user account, used day-to-day for non-administrative tasks, should not have any elevated privileges.

Single Sign-On (SSO) is convenient and secure when an enterprise has many applications, including cloud applications, which helps reduce the number of passwords a user must manage. Users are recommended to use password manager applications to securely store their passwords, and should be instructed not to keep them in spreadsheets or text files on their computers. MFA is recommended for remote access.

Users must also be automatically logged out of the system after a period of inactivity, and be trained to lock their screen when they leave their device to minimize the possibility of someone else in physical proximity around the user accessing their system, applications, or data.

An excellent resource is the NIST® Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

For guidance on the creation and use of passwords, reference the CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-password-policy-guide

Safeguards

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Asset Type: Users	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.2: Use Unique Passwords

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Safeguard 5.3: Disable Dormant Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts

Asset Type: Users	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.6: Centralize Account Management

Asset Type: Users	Security Function: Govern	IG2 IG3

Centralize account management through a directory or identity service.