Identity Management Day

April 3, 2024

Identity (ID) Management Day aims to inform about the dangers of improperly managing and securing digital identities, by raising awareness, sharing best practices, and inspiring individuals and organizations to act.

Established in 2021, in partnership with the National Cybersecurity Alliance (NCA), ID Management Day is a day to educate business leaders, IT decision makers, and the general public about the importance of identity management. It is celebrated annually on the second Tuesday of April, which is April 9 th for 2024.

What is ID Management?

ID Management is the organizational process to ensure individuals have the appropriate access to technology resources. It involves a careful review of each user's role and responsibilities.

Only the necessary rights and resources should be assigned to each user. These privileges should be periodically reviewed and adjusted as needed.

Why is it important?

Cybersecurity incidents involving compromised identities continue to be the most common cause of a data breach for businesses, and account takeover for individuals.

- 84% of organizations suffered an identity-related breach and 78% experienced direct business impacts (Identity Defined Security Alliance).
- Account takeover attacks increased by 354% year-over-year in 2023 (Sift’s Q3 2023 Digital Trust & Safety Index).

Principles of ID Management

Below are six key principles to ensure ID Management systems are efficient and secure.

Principle of Least Privilege (PoLP)

Gives users the least amount of privileges necessary to perform their job functions. This minimizes exposure to sensitive information and reduces the risk of data breaches. Only the necessary rights and resources should be assigned to each user.

Role-Based Access

Manages access to resources based on the roles of individual users, within an organization. Instead of assigning permissions to individual users, permissions are assigned to roles, and users are assigned to these roles. This streamlines the administration of access rights and ensures users only have access to the resources they need for their roles.

Zero Trust

Assumes nothing inside or outside an organization can be trusted by default. This means continually verifying every access request to ensure it is fully authenticated and authorized before access is granted. Trust must be earned, not assumed, and it must be re-earned with each new access request.

Single Sign-on

Allows users to log in once and gain access to multiple applications or systems without needing to log in again. This not only enhances user convenience but also reduces the risk of password-related security breaches.

Multi-Factor Authentication (MFA)

Requires more than one method of authentication, from independent categories of credentials, to verify the user’s identity. These methods could be something the user knows (like a password) or something the user has (like a fingerprint).

MFA adds an extra layer of security and makes it harder for unauthorized users to gain access. Even if a bad actor manages to acquire a user’s password, they would also need the additional factor(s) to access the system.

Password Policies

Rules designed to enhance security by encouraging users to create reliable, secure passwords, and use them properly. These policies may require users to change their passwords regularly, avoid using easily guessable passwords, and use a mix of characters in their passwords.

McLennan Community College (MCC) continues to improve cybersecurity across campus. We will continue to educate and communicate as we progress in these areas.

Revision #1
Created 12 December 2024 19:01:03 by Laura J. Crapps
Updated 12 December 2024 19:01:30 by Laura J. Crapps