Jackie Lutz
(201) 815-6240
jackienlutz@gmail.com

Explain what multifactor authentication is, how it can be used, and how it can reduce risk to an organization.

Multifactor authentication (MFA) is a layered process designed to protect an account user's data. It requires two or more authentication methods to validate a user's identity. This process is used to protect the user's data from security threats, and is more secure than just using a password.

MFA can be enabled for most online services. One commonly used form of MFA is through text or voice message. To enable this, the user provides their phone number to the online service. When the user attempts to log in to an account with this form of MFA enabled, they are prompted to verify their identity by checking their phone. They receive a message containing a code to use to log in. This provides multiple layers of protection for the user's data and identity.

The Cybersecurity and Infrastructure Security Agency (CISA) provides a multifactor authentication hierarchy, which ranks the forms of MFA from least to most protective. The least protective form is through SMS or voice authentication, while the strongest form is through Fast Identity Online (FIDO) authentication. FIDO is a phishing-resistant form of authentication, and is based on public key cryptography. This replaces the password login process with passkeys. Passkeys can be used for multiple devices. They allow for the user to sign in with the same biometric or pin that they used to sign in to their device initially.

MFA reduces the risk of security breaches for the organization and the user. Even if passwords are compromised, MFA will provide extra protection. Recently, many companies have transitioned to a remote or hybrid approach. Adaptive multifactor authentication allows for organizations to choose what factors a user experiences when logging in, based on multiple variables. For example, if the user is using wifi from a public library rather than their home network, the MFA will detect this. As a result, it may require them to log in using multiple methods of authentication. This decreases security risks for organizations.

MFA also offers single sign-on (SSO), which is a one-step authentication method that allows users to log in to multiple applications at once. This is convenient for organizations, since their employees will spend less time logging into each application and more time getting tasks completed.

MFA increases security for users and organizations, and streamlines access to applications. In the modern online environment, the use of MFA is essential for keeping sensitive data protected from security breaches.

Sources:

"More than a Password: CISA." Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/MFA. Accessed 16 May 2024.

"Passkeys (Passkey Authentication)." FIDO Alliance, 16 May 2024, fidoalliance.org/passkeys/.

"What Is Fido." FIDO Alliance, 7 Mar. 2024, fidoalliance.org/what-is-fido/.

"Why Multi-Factor Authentication (MFA) Is Important." Okta, www.okta.com/identity-101/why-mfa-is-everywhere/. Accessed 16 May 2024.

Yasar, Kinza, and Mary E. Shacklett. "What Is Multifactor Authentication?: Definition from TechTarget." Security, TechTarget, 2 Oct. 2023, www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA.