Steps for effectively deploying multi-factor authentication (MFA)

CANADIAN CENTRE FOR CYBER SECURITY

May 2023 | ITSAP.00.105

Threat actors commonly exploit weak or stolen credentials to compromise accounts, allowing them to breach your network, take control of your systems, and gain access to your sensitive information. To increase your organization's resilience to these cyber attacks, you should use strong authentication mechanisms, primarily multi-factor authentication (MFA), to secure accounts and devices on your networks. MFA can provide enhanced security whether you operate in an on-premise (on-prem), cloud, or hybrid environment.

MFA requires a user to provide two or more different authentication factors to verify their identity during a login process. These authentication factors can be a combination of something the user knows (e.g. password or PIN), something the user has (e.g. a smart card or a security key), or something the user is (biometric features e.g. fingerprint or face scan). MFA, especially when used with other security controls, provides higher assurance that only the authorized people have access to the right resources. This guidance can help your organization to effectively deploy MFA as an additional layer of security to reduce your risk and likelihood of compromised credential attacks or data breaches.

Best practices for deploying MFA

To ensure a successful MFA deployment you need a plan. Start by consulting stakeholders across your organization and identify the organizational assets (high business value or sensitive systems and data) you need to protect. Work to understand the negative impacts of implementing an MFA solution on your users so that you can proactively plan mitigation measures. Select an MFA solution that fits your organizational requirements and can be scaled to meet your organization's needs as it grows and evolves. Consider that your organization may require a number of MFA solutions, for example, to meet a variety of needs for different users such as internal administrators, regular users, and external clients. Be aware that not all MFA solutions are created equal. Many of these solutions offer different functionalities and some may have more secure MFA implementations than others. Regardless of the MFA solution you choose, your organization can deploy MFA effectively by adhering to the following best practices.

Prepare your users to minimize potential pushback and greater acceptance of MFA

- ☐ Run awareness campaigns in advance to explain how MFA will protect their accounts and improve the organization's overall security.
- ☐ Provide user training sessions to enhance their understanding of the new authentication methods.
- ☐ Educate users on identifying, reporting, and mitigating social engineering attacks, such as phishing and MFA spamming. Sometimes called MFA fatigue, it's a technique where threat actors flood the target user with notifications pushed over the phone, email, or messaging platforms to accept the MFA prompt. Users should be trained to call and report this issue to your IT department as soon as possible.

Plan a phased-in roll out to improve your organization's cyber security as soon as possible

- ☐ Enforce MFA initially for accounts that are high-value targets for threat actors to protect against misuse of privileged accounts and important business communications. This include administrative accounts and email accounts of senior management.
- ☐ Consider running a pilot deployment involving user groups with varying levels of security access. Use the lessons learned from the pilot to fine tune the final deployment plan to the rest of your organization.

Develop sign-on policies that meet the needs of your organization and the sensitivity of your data

- ☐ Consider using MFA for all users, systems, applications (on cloud and on-prem), and endpoints on your network. At a minimum, enable MFA for accounts associated with sensitive data such as those containing financial records and personally identifiable information (PII).
- ☐ Apply risk-based conditional access so that additional authentication methods are required as the level of risk of compromise to access a system increases.
- ☐ Understand your regulatory compliance requirements and tailor your MFA solutions accordingly.
- ☐ Set up session-based MFA policies for high-risk logins so users must enter their credentials when their timed session expires. User credentials should be continuously validated on each re-login.
- ☐ Require additional authentication factors based on context such as the user's role, location, or behaviour. It could also be based on the risk level of the intended task. For example, users working remotely would have different MFA factor requirements than users in the office.

Prepare your infrastructure for the MFA deployment. Update software or hardware components, test the systems, and make sure that nothing will break if MFA required changes are applied.

Communications Security Establishment | Centre de la sécurité des télécommunications

Cat. No. D97-1/00-105-2023E-PDF ISBN 978-0-660-48612-3

Canada

Steps for effectively deploying multi-factor authentication (MFA)

Choose the appropriate MFA factors based on the level of protection required

- □ Implement hardware-based MFA that is independent of the device being authenticated. For example, fast identity online (FIDO) based-solutions are strongly recommended to secure online accounts. Check out the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) publication on Next Level MFA: FIDO Authentication.
- □ Require the use of authenticator applications, security keys, or smartcards as extra authentication factors when users are accessing the corporate network via a company authorized device.
- □ Only consider short message service (SMS) codes as an authentication factor for low-risk logins. SMS is insecure as codes are sent in unencrypted form. An increasing number of cyber attacks involves threat actors intercepting SMS codes through SIM swapping, phishing or other social engineering attacks.

Balance user experience and security protection to maximize security and minimize disruptions

- □ Allow users flexibility to use different types of factors, where possible, such as security keys, biometrics, or PIN. This can empower your users to have a choice and provide convenience for them that could increase greater acceptance of MFA.
- □ Provide a mechanism for users to provide their feedback on their MFA experience and be open to adjusting your policies and procedures to improve user experience. The feedback mechanism can help to reveal user comfort issues, for example privacy concerns with some types of MFA like biometrics.
- □ Implement MFA with a single sign-on (SSO) application to automatically log authorized users into their connected accounts. This can improve user experience as it saves them from logging into multiple accounts each day.
- □ Conduct regular assessments of your MFA solution to ensure that it continues to meet your users' needs and protects your organization's sensitive information. This is important as cyber security technologies change.

99.9% of account compromises can be blocked with MFA

According to 2019 study by Microsoft

Reduce the burden on IT resources when supporting the roll-out and maintenance of MFA

- □ Provide users with a backup MFA factor that is identical in strength as the primary one. Set up an easy way for users to reset them on their own in case their primary factor is lost, unavailable, or compromised.
- □ Use associated monitoring tools to automatically detect and block suspicious IPs accessing your network.
- □ Enable event logging of MFA events and monitor authentication reports. This allows you to detect anomalous attacks which may seek to exploit gaps in the onboarding and/or revocation process.
- □ Use auditing tools to assist with troubleshooting and adjusting MFA policies based on usage.
- □ Allow users the ability to disassociate a lost or stolen device/security key from their account. This prevents threat actors from accessing the user's account if the stolen device falls into the wrong hands.
- □ Set up emergency or "break glass" account(s) for managing administrative activities especially in cases when the MFA authentication mechanism become unavailable. Emergency account credentials should be strictly secured and only used as part of an incident management process.

For more information, check out the following resources:

- Don't take the bait: recognize and avoid phishing attacks (ITSAP.00.101)
- Secure your accounts and devices with multi-factor authentication (ITSAP 30.030)
- Best practices for passphrases and passwords (ITSAP.30.032)
- User authentication guidance for information technology systems (ITSP.30.031 v3)
- Authentication methods: choosing the right type (National Cyber Security Centre)
- Use strong user authentication eLearning course (Innovation, Science and Economic Development Canada)
- More than a password - protect yourself from malicious hackers with multifactor authentication (Cybersecurity and Infrastructure Security Agency)

Cat. No. D97-1/00-105-2023E-PDF ISBN 978-0-660-48612-3