Multifactor authentication (MFA) is an integral component of cybersecurity. By requiring additional steps to access data, information is more secure and harder to steal. However, cybercriminals have developed new ways to break through these cyber defenses. This category of attacks, known as MFA bypass attacks, puts businesses at risk of data breaches, which can lead to significant expenses and reputational damage.

Organizations of all sizes are vulnerable to MFA bypass attacks and must implement protective measures to safeguard their data. This article provides an overview of MFA and MFA bypass attacks, discusses common methods used in MFA bypass attacks, and offers strategies that employers can use to mitigate the risk of these cyber incidents.

Authentication is a security protocol that requires users to verify their identity through a specified process (e.g., entering a username and password). As cyberthreats have emerged and evolved, additional layers of protection have been added through MFA. This security method requires more than one "factor" to validate a user's identity. The three most commonly used factors in MFA are:

1. **Something a user knows**, such as a PIN or a password
2. **Something a user has**, such as a mobile device
3. **Something a user is**, such as their biometric data (e.g., fingerprint)

By requiring multiple layers of verification, a system and its data are exponentially more secure. This is because threat actors would have a harder time acquiring the factors necessary to access them.

Although MFA provides heightened security, it still contains vulnerabilities; threat actors have devised ways to defeat these security measures. These MFA bypass attacks exploit weaknesses in MFA implementations and allow cybercriminals to access a business's sensitive data. These breaches can substantially impact a business financially by making them pay fines, legal costs and remediation expenses. Cyberattacks can also cause business interruptions, leading to a loss of valuable revenue during the downtime. Additionally, cybersecurity events can damage stakeholder and client trust, negatively affecting the organization's reputation.

Threat actors employ numerous techniques to bypass MFA security measures. Common tactics include:

- **Malware attacks**—Cybercriminals may utilize malware, or malicious software that is unsuspectingly loaded onto a computer system, to conduct an MFA bypass attack. Once a device has been infected, threat actors can access it and obtain passwords through keylogging, steal session tokens and capture one-time passcodes.
- **Man-in-the-middle (MITM) attacks**—These incidents involve a hacker intercepting communications between the user and the authentication system, allowing them to capture MFA tokens or credentials, especially if the connection is not properly encrypted.
- **Phishing attacks**—These attacks occur when cybercriminals use fraudulent electronic communications (e.g., emails) or cloned websites to trick users into providing their credentials, including MFA tokens.
- **SIM swapping**—This tactic involves an attacker transferring a victim's phone number to a new SIM card, enabling them to intercept MFA codes. This allows the threat actor to fraudulently approve MFA requests on their device.

- **MFA push attacks**—In this scheme, cybercriminals take advantage of users' tendencies to accept push notifications. After a threat actor has obtained a user's login information (e.g., username and password), they may send out numerous fraudulent push notifications with the hope the user either grows tired of them or mistakenly believes them to be a glitch, so they accept the request.

With the emergence of MFA bypass attacks, employers should implement protective measures to defend against them. The following are strategies to consider:

- **Utilize phishing-resistant MFA**. Employers can use robust authenticators, including hardware security keys, biometric identifiers and direct communications, to strengthen their cyber defenses against phishing attacks. These types of authenticators are more difficult to compromise, duplicate or intercept than simpler ones.
- **Require strong, nonreusable passwords**. Employers should require strong passwords to guard against brute-force hackers who may repeatedly try to guess a password by using multiple combinations of letters and numbers. They should also forbid reusing passwords for different accounts so a compromised password doesn't grant access to multiple networks.
- **Implement zero-trust security models**. Building a zero-trust security framework can help prevent MFA bypass attacks by continuously verifying users and devices throughout a session rather than relying only on the initial login.
- **Have strong access controls**. Organizations should limit the number of users that can access sensitive information. This reduces the number of individuals a threat actor may target.
- **Educate users**. As cybercriminals continually develop new ways to exploit weaknesses in cyber defenses, employers should provide ongoing training on recognizing and responding to phishing attempts and how to report suspicious MFA requests. Employees should also be educated on the importance of keeping their devices (e.g., cellphones) secure, not leaving them unattended and what to do if they are lost or stolen.
- **Conduct regular audits and tests and continually update security**. Employers should perform regular security audits and penetration tests to find vulnerabilities in their cybersecurity defenses. They also need to ensure procedures are in place to continually update and patch their systems.
- **Secure cyber insurance**. Employers should obtain a cyber insurance policy that addresses losses that could arise following an MFA bypass attack or another cyberattack. Such losses may include costs related to data breaches, legal liabilities and incident response services. An insurance professional can help businesses find the policy that best suits their needs.

Cybercriminals have developed ways to infiltrate networks and systems, even when MFA is utilized. To ensure sensitive information remains protected, businesses must implement robust security measures that address this risk. Doing so can help stop these attacks, preventing associated financial losses and reputational damage.

Contact us today for more information.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.
[b_disclaimer]