Prescient Solutions

Enhancing IT Security Through Multi-Factor Authentication

GUIDE

Protecting against data breaches requires strong access controls that secure sensitive systems and data from unauthorized access. Login credentials are a top target of hackers, and those stolen credentials are a leading cause of data breaches. Combine those facts with the ongoing increase in the number of breaches, and it's clear that existing means of credentialing users and protecting their credentials needs to improve.

Passwords are Weak Credentials

The traditional security credential, a password, dates back before the invention of the computer. But relying on just a password is problematic for several reasons:

Passwords

- **Passwords are weak.** Because of the difficulty of reliably keying in a lengthy password, most users rely on short passwords. These short passwords are easily broken by brute force attacks. Several years ago, that required only a few hours. With today's more powerful CPUs, it's more likely to be a matter of minutes.

- **Passwords aren't secure.** Users can't remember passwords, so they write them down or store them in files on their computers. Users often base their passwords on personal information, including names and dates related to family members and pets, so someone who knows the user or follows their social media activity may be able to guess their password. Their personal information may also be for sale on the dark web, helping bad actors to guess at passwords.

- **Passwords aren't confidential.** In an effort to help out their colleagues and to avoid delays if a password needs to be reset, users often share their passwords. Functional accounts for operations may be shared and may still use the default password set by the vendor. In addition, the dark web is full of sites offering user credentials for sale, cheap—passwords for non-financial institutions may sell for as little as $1.

- **Passwords aren't unique.** Even when a company's password policy prohibits reusing passwords, it can only enforce the rule within the organization. Because passwords are so hard to come up with and to remember, users frequently reuse the same password across multiple sites. When one site is breached, hackers know to try the same credentials on other sites, too.

- **Malware can capture passwords.** Phishing scams and malware allow hackers to capture passwords as users type them into login forms. The risks have grown as users increasingly work from home and other off-site locations, where corporate security controls may not apply. Users working on home devices may not have the latest security patches installed, and users working in coffee shops may use insecure networks, allowing bad actors to secretly install password-capturing software on their devices.

Multi-Factor Authentication Backs Up Passwords with Another Authentication Method

Because of these weaknesses in passwords, it's dangerous to rely solely on passwords for users to prove their identity. Multi-factor authentication (MFA), most commonly set up as two-factor authentication, requires additional identity checks for proof of identity. By having to satisfy two different checks, the risk of credentials being compromised is reduced. It's important to note that the two different checks need to use two different methods to provide additional security. Requiring a user to answer a security question is simply asking the user to enter a second static password and does not enhance security.

Effective multi-factor authentication requires users to satisfy two or more identity checks from different categories of proof, including:

- Something you know, such as a password, pin, or security question.
- Something you have, such as a phone, token, or smartcard.
- Something you are, using biometrics such as fingerprints, voiceprints, or retinal scans.
- Something you do, including gestures and typing patterns.
- Somewhere you are, such as an authorized location or IP address at an authorized time of day.

Combining "something you know" with "something you have" is by far the most common implementation of two-factor authentication. That's more secure than a password alone, but neither is actually proof of identity. Biometrics provides true proof of identity, but users may be hesitant to have such data stored.

Multi-factor authentication

Multi-Factor Authentication Has Risks and Limitations

Although using two or more different authentication methods prevents hackers from simply stealing or guessing passwords to gain access, MFA has its own vulnerabilities that hackers can leverage to get around the additional controls. These weaknesses include:

- **Lost phones reveal login codes on the lock screen.**
Sending text messages to cellphones to deliver a one-time password is very common. However, phones can be lost or stolen, and text message notifications containing login codes can simply be read off the lock screen.

- **Attacks intercept SMS messages.**
A user doesn't have to lose their phone to lose control of text messages containing login pins. Hackers may be able to attack the cellphone network and see SMS traffic. Hackers can also attack cell service providers and forward calls and messages to their own devices. Finally, hackers can transfer a user's phone number to a SIM card owned by the hacker.

- **Token-generating devices can be lost.**
Like phones, key fobs and smart cards can easily be lost. Depending on whether the device has its own protection, it may be possible for anyone who picks up the device to access the one-time password.

- **Social engineering.**
Hackers can use several methods to trick users into revealing passwords. Links in email can redirect users to login pages that are intercepted by the hacker's site, allowing the hacker to steal the session cookie and gain access. In another approach, a hacker will click on the "reset password" link for a user's account and then call the user, posing as the business's security team, and ask them to "verify" the security code that was sent.

- **Poor employee security practices.**
Some MFA processes allow users to simply click a link rather than enter a one-time password into a login page. If a hacker is attempting to login and triggers these prompts, an employee can accidentally click the verification link, granting entry to the hacker.

- **Implementation errors.**
MFA can be implemented incorrectly. In some incorrect implementations, the second authentication step can simply be bypassed.

In addition to vulnerability to attacks, other limitations of MFA include:

- **Loss of access.**
Users who lose their phone or token generator lose access to systems until the device is replaced. If access rights are based on patterns of usage or keyboarding, those patterns can change for legitimate reasons—travel; a broken finger—and prevent a user from gaining access.

- **Multi-factor authentication is annoying.**
Security measures need to be balanced against user satisfaction. Having to pass two verification checks is frankly annoying to many users. In order to discourage users from trying to find ways to bypass these checks, limit use of MFA to access coming from outside the corporate network or coming into highly sensitive systems.

Incorporating Multi-Factor Authentication into Access Controls

Despite the limitations, MFA adds a valuable additional layer of security and should be incorporated into layered security and defense in depth strategies. Activating multi-factor authentication for Microsoft cloud services is reported to reduce the risk of an account being compromised by 99.9%. Assuming that a similar level of benefit applies elsewhere, MFA offers one of the most effective security measures available.

To make multi-factor authentication effective, take these steps:

- **Use where it makes sense.**
Apply MFA to protect cloud-based resources and to protect internal resources that are accessed from outside the corporate network. Also use MFA to protect highly sensitive systems and sensitive network segments inside the corporate perimeter, even when being accessed internally.

- **Apply other identity controls.**
MFA isn't the only identity-related control needed to protect systems. Use role-based privileges to ensure that once users are granted access, they can only access systems and perform functions that match their job responsibilities. Use federated identity systems where possible to ensure that user data and privileges are consistent across all locations.

- **Utilize other security software.**
Continue to use tools such as firewalls, intrusion detection software, data loss prevention software, and antivirus software to protect against malware and attacks.

- **Keep patches up to date.** Help protect users and systems against malware by deploying security patches in a timely matter.

- **Implement appropriate monitoring.** Use analytics software to identify unusual patterns of access that can indicate an attack. Ensure logs are periodically reviewed manually as well as relying on automated alerts, and make sure alert triggers are refined so teams aren't overwhelmed by false alarms and conditioned to ignore alerts that may indicate a real problem.

Prescient Solutions helps businesses in the Chicago and Schaumburg areas implement comprehensive information security strategies.

Contact us to learn more about using multi-factor authentication to protect your business.

Prescient Headquarters
1515 Woodfield Rd, Suite 880
Schaumburg, IL 60173
Phone: (847) 240-3900

About Prescient Solutions

Prescient Solutions has been providing managed technology services both on site and remotely to small, medium and large enterprises and government agencies for 20 years. With certifications in key technologies spanning hardware, software, network, security, and other specializations, our team has the insight and experience to address the technical challenges that are holding back your IT team and your business. For more information about Prescient Solutions, or to request a complimentary IT consulation, call 888-343-6040, or visit www.PrescientSolutions.com.