Modern Adaptive Multi-Factor Authentication

Introduction

Cybersecurity attacks are escalating at a rapid pace and organizations are expanding their use of cloud and mobile apps at almost the same tempo. As such, Information Technology (IT) and security professionals are struggling with the daunting task of protecting critical company information. As most data breaches involve stolen or weak identity credentials that were acquired through phishing attacks, simple password protections are no longer adequate. The Symantec April 2017 Internet Security Threat Report reveals that over the last 8 years, more than 7.1 billion identities have been exposed in data breaches.

Today, organizations need to augment the capabilities of traditional Identity and Access Management (IAM) by employing Multi-Factor Authentication (MFA) that ensures adequate protection and compliance through seamless authentication across all applications. Best-in-class MFA should authenticate identities with the desired level of assurance, and bear in mind that different user types have entirely different risk profiles which require fundamentally different approaches to authentication. Administrative staff might be subjected to fewer controls and more leniency, whereas high-risk 'access employees' may have higher identity assurance thresholds. Additionally, effective MFA should include adaptive functionality with the ability to challenge for step-up authentication based on user or device context.

Cybersecurity Landscape

The challenges related to implementing effective IAM, along with the consequences for failure, are increasing dramatically. A 2016 Cost of Data Breach study from the Ponemon Institute estimates that the typical cost for one breach is now $4 million, but that's just the tip of the iceberg. The U.S. and most international governments, as well as virtually all U.S. states and foreign territories, have mandates that include hefty fines, public disclosure requirements, and the allowance of lawsuits by affected parties. In many cases, complying with standards and regulations such as NIST, NYDFS, PCI DSS, HIPAA, FINRA and many others require the use of advanced security methods that transcend legacy authentication. In fact, most compliance standards now require secure access beyond single-factor authentication—or the use of simple passwords. Given the increases in the frequency and severity of breaches, and the proliferation of phishing and hacking incidents, improving identity validation has become one of the most critical steps that IT and security professionals can take to decrease security risks.

Identity Challenges

User credential theft is one of the most pressing security challenges today as it can provide the keys to an organization's kingdom. As verified by the 2017 Verizon Data Breach Investigation Report, more than 80% of data breaches involve stolen or weak identity credentials. Privacyrights.org has documented that over the past few years, 893 publicly acknowledged breaches resulted in over 172 million lost records. Protecting user credentials has become a high priority for most organizations. Once a user's credentials have been compromised, an attacker has access to a host of internal resources. They can pose as an employee to gain additional credentials, increase privilege levels, and steal or compromise valuable information.

The Verizon report also shows that user credentials are targeted in over 90% of phishing attacks. These attackers frequently use sophisticated phishing and spear phishing attacks using advanced social engineering techniques to compromise users. Even though many organizations are trying to better educate their users about these attacks, credential phishing is still rampant. To steal user credentials, hackers are using cleverly disguised phishing emails, text messages, and other techniques. A leading email cybersecurity firm discovered that 25% of these emails target Apple IDs, with Microsoft Outlook and Google Drive credential targeting as second and third on the list, respectively. Lack of user training, combined with escalating email phishing sophistication, has given rise to cybercriminal campaign click rates.

User passwords continue to pose huge problems for IT and security teams. In most organizations, users duplicate almost three-fourths of their passwords. Typically, these users only have a handful of passwords that are often weak and easily hacked. Once hackers discover a single password, they can exploit this knowledge to gain access into a variety of systems and applications that contain sensitive and critical information. This vulnerability exposes firms to serious consequences including ransom demands, brand damage, customer declines and

regulatory fines. Solving the password dilemma has become one of the more important enterprise challenges today, prompting many organizations to consider solutions that eliminate the need for passwords altogether.

IAM Best Practices

Authentication is often based on two assumptions that may not be correct: One, that users create effective passwords. As noted above, this is usually not the case. Two, that secret passwords are known only to users so they can't be hacked. In reality, hackers can now easily crack or steal passwords. To solve these challenges, organizations are implementing Multi-Factor Authentication (MFA), which uses multiple data points and factors derived from a login attempt, such as device and location context, to verify identity and prevent access based on simple passwords alone. By employing MFA, IT and security teams can help ensure that hackers can't penetrate the enterprise with a single stolen password.

The best type of MFA is Adaptive MFA as it can integrate a firm's applications and resources to add a layer of authentication. With AMFA, every time a user logs in, the system will analyze the request via backend analytics to determine how much access to grant.

For example, if an employee is on-premises at an office location, based on approved network settings and security policies, AMFA will recognize that this is a secure location and set the appropriate level of authentication. AMFA can also recognize if the user is attempting to authenticate from a previously authenticated device and adjust accordingly. If a user tries to authenticate from an offsite or unrecognized location, the system will step-up authentication by challenging with a second factor to validate identity.

To ensure optimal IAM security, Okta recommends evaluating a potential AMFA solution against three macro requirements:

Requirement #1: Simple

The best MFA solutions offer ease-of-use and implementation via a non-disruptive, non-intrusive, easily integrated solution that works with your existing infrastructure and VPNs. It should also provide simple and intuitive management and monitoring.

Three things to consider include:

- Usability and better overall experience for users with low-touch authentication and third party integration for alternative factors; support for biometric access with fast fingerprint Touch ID
- Phased deployment with easy centralized administration and management to ensure regulatory compliance across all applications and services
- Flexible administration consoles to allow IT professionals to adjust password lengths and complexities and update schedules

Requirement #2: Secure

Your MFA solution should offer the ultimate protection while helping you meet all the standards and mandates required under current and new regulations. It should also help you avoid other security-related consequences such as lawsuits and fines while eliminating costly disruptions and user complaints.

Three things to take into consideration include:

- Full range of factor and assurance level support including crypto-based factors (OTP, security tokens, etc.)
- Adaptive functionality with challenge for step-up authentication for additional security without overburdening users
- Secure authentication for on-premises, cloud, and mobile applications with Verify and Verify Push smartphone apps

Requirement #3: Extensible

A best-in-class MFA solution must be extensible to allow for improved productivity and faster return on investment. The best solutions include compatibility with third party solutions and industry-proven reliability.

Here are three things to consider:

- Single solution extensible across the enterprise (Cloud, SaaS, on-premises, legacy); integration with custom applications with API support for unique use cases and needs
- Works with existing security tools to extend investments, provides meaningful authentication data, supports RDP, VPN, and a broad set of systems in the data center
- Enables visibility and response, especially when integrated with other SIEM and security tools; ensures action can be taken (e.g. limit/revoke account access) based on events

Conclusion

Organizations today are augmenting their IAM posture and solutions by adding Multi-Factor Authentication that provides enhanced cybersecurity protection and ensures regulatory compliance. Optimal MFA solutions should include secure adaptive functionality with step-up authentication, simple implementation and ease-of-use for administrators and users, and extensible flexibility across the entire organization and security stack.

Adaptive Multi-Factor Authentication should be enabled throughout your organization to help eliminate the use of vulnerable passwords. Implementing AMFA for everything everywhere can also eliminate identity sprawl via Single Sign-On in place of cumbersome approaches that inhibit productivity. The best Adaptive MFA solutions help you identify potential account compromises and accelerate attack responses via robust ecosystem integrations. Employees will be thrilled by the elimination of password management, which is a difficult daily task. Now you can implement secure IAM that includes a federated architecture that's everywhere your employees are, including cloud, mobile and on-premises. When attackers try to breach your firm with credential phishing, AMFA provides technical controls at the email gateway and a reduced attack surface via secure user identity.

Best-in-class Adaptive MFA authenticates identities by providing the desired level of assurance and verification. While many solutions deliver a variety of verification capabilities, the best solutions manage identities as a core component of the platform.

Along with Adaptive MFA, sophisticated lifecycle management can ensure orchestration and entitlement management to maintain the optimal level of access to your applications. You can easily set access and entitlement rules based on attributes, such as user group membership, and provide visibility into who has access to what data through simple access governance.

IAM Best Practice Considerations

Simple

- Usability and better overall experience for users
- Ease of management for administrators
- Phased deployment for easy onboarding

Secure

- Verify and Verify Push smartphone apps and biometric access
- Adaptive functionality with challenge for step-up authentication
- Anomaly detection, device trust, dynamic IP blacklisting, and more

Extensible

- Supports a wide range of applications and environments
- Extensible and integrates with business applications and existing security tools
- Robust reporting and API to monitor authentication events