Strategies to Mitigate Cyber Security Incidents

okta

Today's Evolving Security Guidelines

Traditional security is insufficient to protect the cloud and hybrid infrastructure of today's enterprise. Our users have adopted new styles of working, and new ways of connecting. As IT becomes nimble—adopting ever increasing cloud solutions—an organisation's sensitive information is everywhere.

Enter digital identity. It's used in nearly every aspect of daily life. The average employee has a multitude of applications and services registered to any one of their personal or business email accounts. At the enterprise, our employees use their identity to access critical data and services now sprawling across cloud, SaaS and on-premises applications. In a post COVID-19 world, this transformation has only accelerated.

Simply updating identity or access tools is not enough. Governments and enterprises need guidance in adopting and implementing today's identity and access management solutions, as part of a comprehensive, organisation-wide security strategy. The Australian Cyber Security Centre (ACSC) has released and updated "prioritised mitigation strategies" to help cyber security professionals in all organisations to evolve and optimise their security posture against a range of threats. These strategies have been recognised across the Australian industry as providing a baseline of security that should be implemented by organisations with the utmost urgency and include guidelines for upgrading Identity and Access Management.

Today's risks require a marriage between security and identity

If the barrage of recent data breaches tells us anything, it's that identity is the new currency in the market. Armies of botnets are attempting to reuse and harvest stolen credentials in drive-by downloads or targeted phishing scams—all while we are still struggling with security basics. The 2019 Verizon Data Breach Investigations Report found that 80% of hacking-related breaches leveraged weak or stolen passwords.[1]

Society's standards around access and identity have been slow to evolve and in turn our authentication strategies have remained stagnant—for nearly 15 years. Passwords are still in use in most organisations and those same entities use multiple solutions to manage access across their sprawling enterprises. This is where the latest ACSC guidelines show a clear path forward.

Identity represents a critical control point that, once addressed, dramatically improves security across the ecosystem. Entities supporting government agencies are now being held to new identity standards, requiring them to take a new look at Identity and Access Management (IAM) in accordance with updated guidelines and mandates. They are looking for a comprehensive solution that understands and meets these requirements.

ACSC Guidelines Address the Changing Risk Landscape

The latest release of the ACSC mitigation strategies has now rated Multi-Factor Authentication (MFA) as 'Essential' to reflect the prevalence of passphrase theft and the abuse of remote access for infiltration, data exfiltration and persistence. As ACSC advises, this applies to VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important data repository.

Across the world, the latest security standards provide similar guidance. In North America, the National Institute of Standards and Technology (NIST) now mandates the use of Multi-Factor Authentication across all federal agencies and government suppliers for privileged access and remote access to the network—essentially applicable to all of today's modern knowledge workers. NIST has recognized, fundamentally, how constantly increasing password complexity has placed all of the security burden on the end user. In its special publication of Digital Identity Guidelines (SP-800-63-3), NIST identifies compensating controls such as MFA as an important way to increase security while reducing complexity.[2] Likewise, the Payment Card Industry Data Security Standard (PCI DSS) requires MFA around applications and infrastructure supporting and processing payment card data.

Mitigating cyber security incidents is easy with Okta

Organizations generally begin with an assessment to identify gaps in compliance across their enterprises. In practice, compliance is often considered cumbersome and costly by many security teams. However, navigating industry-leading guidance for authentication and identity management is Okta's business. Okta's cloud-native access management centralises IAM and offers a full range of factor and assurance level support across standard identity categories.

Though Okta's solutions do not span across all ACSC mitigation strategies, Okta offers a centralized solution to meet your security and compliance needs around IAM. Key Okta attributes/capabilities include the ability to:

- **Centralise identity management** throughout the ecosystem,
- Implement **simple authentication** that is adaptive, risk-based and flexible,
- Reduce your attack surface with **automated lifecycle management**, and
- Enable **visibility** and **response**

Centralise identity management throughout the ecosystem

Regardless of compliance or business need, Okta ensures strong authentication across all services, everywhere. Workday, Microsoft Office 365, Salesforce, etc. Okta integrates seamlessly with the applications you are already using. The Okta Identity Cloud uses standards-based protocols and API's to integrate with over 7,000 applications, IT infrastructure, and devices. Our federated architecture is recommended by the latest NIST guidelines and is fully compliant with 800-63C's Identity Federation and Assertions recommendations.[3]

Identity management doesn't start and stop at the enterprise cloud services and neither does Okta. You can secure existing on-premises infrastructure with the same IAM from Okta. Supported by rich SAML, your cloud IAM can be your primary IAM with delegated authentication to AD or LDAP and third party IDP. Connect to a broader set of systems in the data centre from RADIUS, Windows Credential Provider, to other infrastructure like Citrix, F5 and Remote Desktop.

Your IT team wants a simple and easy management that includes out-of-the-box integrations with a variety of applications, custom application integration options, phased deployment options, and centralised administration and management to ensure compliance across all applications and services. You need to reduce identity sprawl and unify under one, federated architecture that can intelligently provide the policy flexibility, automation, and intelligence to meet the demands of identity management in today's enterprise.

Implement simple authentication that is adaptive, risk-based and flexible

Okta sets a new baseline with two-factor authentication across all solutions. Not just through the use of step-up security or added protection around critical infrastructure or services, Okta adds a simple one-time passcode to every Single Sign-On user so that two-factor authentication is now the authentication for every Okta user.

Context-driven protection

Okta's MFA is adaptive in addressing the entire digital profile including the user, device, and network. Okta's Identity Cloud monitors behaviours and detects anomalies in access behaviour. Is the user attempting to connect from an unknown device? Are they on a trusted network or out-of-band? With this information, your team can dynamically adapt security and authentication policies to enforce step-up authentication for each individual user and situation. Further, Okta's new device login notification informs the user when an unknown device or browser attempts to connect.

Factors for every situation

Okta's Adaptive MFA enables robust features that not only meet standards recommendations but strengthen access and authentication across all users, applications and devices. Okta's Adaptive MFA meets latest industry guidelines and can help customers achieve Essential Eight Level 1, 2 & 3 maturity by enabling a comprehensive set of second factors shifting away from SMS-based verification to stronger options offered by mobile apps, biometrics and unique PINs. The Okta Verify smartphone app allows users to authenticate with ease of use that is as simple as a tap acknowledgement from the user. Okta MFA also supports biometric access with Touch ID, and Windows Hello.

Flexible to meet users' needs

The latest advice from ACSC around passwords, PINs and passphrases focuses on password complexity rules. Okta's flexible admin consoles allow IT to adjust password length, complexity and update schedules to meet this new paradigm. Further, you can enable Okta's Common Password Detection to meet latest guidelines and improve your users' password origination. Common Password Detection will detect and prevent users from defining weak or easily breached passwords.

Reduce your attack surface with automated lifecycle management

Okta allows you to easily and simply create a more defensible perimeter for the whole organisation and protect against unauthorized access. Centrally manage the cycle of events in your users' identity from enrolment, to evolving access across systems and services, to renewal and termination. Managed consistently across enterprise services affords the greatest compliance with key controls.

Accurate entitlement and automated on- and off-boarding

Okta is centrally managed and automated which helps to ensure accurate entitlements and allows you to scale provisioning/deprovisioning across all users, groups, and permissions policies. On-boarding becomes turnkey. Administrators have at-a-glance visibility into users' access to every app, service and data store.

Reduce the risk of lateral movement

Better management not only equates to compliance but improved security. Reducing over-privilege and orphan accounts shrink your attack surface. With Okta, you gain assurance that each account has the right level of access, assigned by policies, and reinforced with step-up authentication based on membership groups and user/device context. Cut the lateral movement by unauthorised users and eliminate privilege escalation.

Enable visibility and response

You have not truly married your IAM with security until you connect directly to your security infrastructure and enable greater visibility and rapid response. With Okta real time authentication, data is accessible by one syslog API. Identity events are seamlessly tied to security management tools like Splunk, ArcSight, IBM QRadar, Palo Alto Networks, and F5 Networks, among others. You will be able to see brute-force or DDoS attacks as they occur. You can take immediate action to challenge account takeover attacks as they occur individually or in multiples across your enterprise. Real-time data from Okta enriches correlation and ultimately enables rapid response. Security teams react immediately reducing containment and mitigation time.

Conclusion

Meeting the latest cybersecurity requirements around IAM does not have to cost tens of thousands of dollars or require months of implementation. The ACSC's Strategies to Mitigate Cyber Security Incidents aim to guide and assist organisations across Australia in protecting their systems against a range of adversaries. The mitigation strategies can be customised based on each organisation's risk profile and the adversaries they are most concerned about. Ultimately, they are security measures that your organisation should already be implementing as part of maintaining a mature security program.

Okta provides a comprehensive solution that allows you to quickly meet the Identity Management and Access Control requirements and seamlessly improve your security posture. Okta offers a solution that immediately meets the most significant hurdle for most organisations. Okta's Identity Cloud and Single Sign-On solution integrates into the applications you are already using in the cloud and corporate data centre. With any Okta solution you not only meet the latest security standards but shrink your attack surface by placing Adaptive MFA in front of literally everything in your enterprise. Lifecycle management is often the largest hurdle in identity management compliance. Okta gives IT admins the central management, policy flexibility, and at-a-glance views they need to efficiently manage the lifecycle of user identities.

Finally, centralizing IAM must include visibility into authentication events in real time. Okta offers flexible data access via native, or API, SIEM integration. Security engineers can take immediate action on events, thwarting attacks before they expand.

Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 7,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device. Thousands of customers, including Culture Amp, Sensis, Xero, Flex, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at www.okta.com

** This white paper discusses certain compliance and legally related concepts, but to be clear, it does not constitute legal advice. If you or your organisation need legal advice, be sure to consult with your own counsel. All content provided in this document is made available for informational purposes only.*

References:

1. Data Breach Investigations Report. Verizon. 2019.

2. Special Publication 800-63-3, Digital Identity Guidelines. National Institute of Standards and Technology (NIST). June 2017.

3. Special Publication 800-63C, Federation and Assertions. National Institute of Standards and Technology (NIST). June 2017.