Security Think Tank: Adopt a Coherent Framework for ID First Security

TechTarget

In this handbook:

Security Think Tank: Adopt a Coherent Framework for ID First Security

ANDREW PEEL

Cyber security models are currently focused on securing relatively static ring-fenced environments of centrally-hosted services. Organisations now face the challenge of transforming those models to manage fluid and scalable environments where their resources and data are distributed across a hybrid mesh of cloud-native and on-premises services delivered by multiple providers.

This new paradigm has resulted in organisations' security perimeters moving from the edge of the corporate network to individual users accessing resources across multiple environments. With identity and access management (IAM) central to enabling secure access to these services, Identity first security has consequently become a key trend in IAM for the cloud.

Unfortunately, many organisations have inadequate IAM controls and don't have effective control of who has access to their resources in traditional static environments let alone the ability to respond to the fast-moving demands of the cloud. As Verizon has reported, more than 60% of breaches in 2021 resulted from hacking using stolen credentials.

In this handbook:

Security Think Tank: Adopt a Coherent Framework for ID First Security

Organisations can effectively manage identities in the cloud by establishing an identity-first security approach. This should combine the use of high quality identity data to provide timely and appropriate access to resources with proactive threat detection and response capabilities.

This should be a core part of an organisation's wider cyber security posture and focus on four elements: identity management, authentication, authorisation and identity threat detection and response.

IDENTITY MANAGEMENT: ESTABLISH AN EFFECTIVE IAM GOVERNANCE FRAMEWORK

An effective IAM governance framework of controls and technology is required to manage an end-to-end identity lifecycle designed to deliver high-quality identity information.

That information informs the provisioning decisions used to provide users with timely and appropriate access to services, and then removes it when it is no longer required. It also offers a single traceable view of who has access to which resources. This is key in the cloud where on-demand access may be required for services from multiple providers.

The provisioned identity information is also used to enable accurate and timely access control decisions, with Identity Providers using it to authenticate access to services, and individuals using it to authorise and enforce the level of access provided to a user.

AUTHENTICATION: ESTABLISH STRONG BUT PROPORTIONATE ACCESS CONTROLS TO REDUCE THE RISK OF ACCOUNT TAKEOVER

For user experience and convenience single-sign-on (SSO) is the authentication mechanism of choice. Unfortunately, many organisations still rely on an insecure mechanism – passwords.

At a minimum, organisations should require the use of multifactor authentication (MFA) tools and techniques. These include mobile authenticator apps leveraging one-time passwords or biometrics combined with controls using contextual signals such as a user's location or the status of their device

Even with MFA, humans and inadequate controls remain a weak point with techniques such as phishing, MFA bombing and ineffective account recovery and device enrolment processes used to compromise credentials. Organisations should combat this through measures such as awareness campaigns on how to identify and

respond to phishing and controls mandating identity verification checks during account recovery.

AUTHORISATION: ENSURE USERS ARE ONLY PROVIDED WITH APPROPRIATE LEVELS OF ACCESS

Organisations need to enforce least privilege models for their cloud resources where users are only provided with the minimum level of access required to do their jobs.

This is dependent on the timely provision to service providers of the accurate, comprehensive and trusted identity attribute data needed to make authorisation decisions. This should include information about a user's role, department, training or clearance levels, combined with robust processes allowing these third parties to decide which of these attributes to use to authorise access.

IDENTITY THREAT DETECTION AND RESPONSE: ASSUME THE PERIMETER WILL BE BREACHED

Although the IAM service does enforce access security, it essentially provides a static defensive perimeter. Organisations must assume this will be breached and use their wider security operations capability to proactively deliver threat detection and response.

Organisations should develop capabilities to detect and analyse signals that could be an indicator of attempted or existing compromise. This can range from brute force or password spray attacks through to signs of unusual user behaviour or privilege escalation. For example, IAM events and signals should feed the SOC's SIEM and SOAR tools to enable it to detect and respond to breaches.

They should also develop the knowledge and capabilities to identify and remove vulnerabilities before they can be exploited. Threat intelligence from cloud-based identity providers could be used to flag at-risk accounts and enable preventative measures to be taken.

Finally, playbooks covering scenarios from containment and eradication through to remediation, need to be in place to guide the organisation's response once a threat has been detected.

Ultimately, organisations need a coherent framework for identity-first security. This will enable them to effectively control access in the cloud by combining the use of high quality identity data to provide timely and appropriate access to resources with proactive threat detection and response capabilities.

Andrew Peel is a cyber security expert at PA Consulting