How Identity and Cloud Governance **Enhances NSA Guidance for Improving Cloud Security**

SailPoint

In late January 2020, the US National Security Agency (NSA) released guidance for **Mitigating Cloud Vulnerabilities**. The document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass many of the known vulnerabilities. It states that cloud customers have a critical role in mitigating misconfiguration and poor access control but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. This eBook provides a summary of its findings and recommendations.

Cloud Components and Threat Actors

The document calls out standard Cloud Service Provider (CSP) architecture components – Identity and Access Management (IdAM), Compute, Networking, and Storage. It states that understanding a CSP's cloud implementation should be part of a customer's risk decision-making process. The document addresses Cloud Encryption and Key Management, Sharing Cloud Security Responsibilities (such as Threat Detection, Incident Response, and Patching/Updating) and Threat Actors; noting that Threat Actors may target the same types of weaknesses in both cloud and traditional system architectures. We have plenty of evidence of this as stated in the document – specifically, identifying the activities of the various types of threat actors – Malicious CSP Administrators, Malicious Customer Cloud Administrators, Cyber Criminals and/or Nation State-Sponsored Actors, and Untrained or Neglectful Customer Cloud Administrators.

Cloud Vulnerabilities and Mitigations

Mitigating cloud vulnerabilities is a shared responsibility between the CSP and the customer organization. Critical to an organization's success in both transitioning to the cloud and maintaining cloud resources is support from informed leadership, which ensures the right governance, budget, and oversight.

Misconfiguration

Misconfiguration of cloud resources is the most prevalent cloud vulnerability and is often exploited to access cloud data and services. Often arising from cloud service policy mistakes, misconfiguration has an impact that varies from denial of service susceptibility to account compromise. The rapid pace of innovation creates new functionality but also adds complexity to securely configuring an organization's cloud resources.

Poor Access Control

Poor access control occurs when cloud resources use weak authentication/authorization methods or include vulnerabilities that bypass these methods. Weaknesses in access control mechanisms can allow an attacker to elevate privileges, resulting in the compromise of cloud resources.

The document mentions that the security principle of 'least privilege' should be applied during initial design and planning and that well-organized cloud governance is also key to a defensible environment.

The stated examples of abused misconfiguration and poor access control are overwhelming and demonstrate the complexities and sophistication of threat actors. NSA provides high-level recommendations for all the vulnerabilities, however, let's take a closer look at the benefits of Identity and Cloud Access Governance and how it enhances risk mitigation for access control and misconfiguration.

Identity and Cloud Access Governance

Managing who has access to what and with which privileges is a real challenge in the cloud due to rapid change and large scale. SailPoint Identity and Cloud Access Governance allow IT and Security Teams to take back control of cloud access by providing 360-visibility across the enterprise and in the cloud and adds a critical layer of security and governance.

Identity and Cloud Access Governance, enables IT to govern access to compute, applications, and data across cloud environments. It does this by protecting and controlling access to resources using policies and guardrails that assure secure, authorized, and appropriate access. By locking down privileged identities and tasks, the risk of excess or stale access and access to sensitive roles is greatly reduced. Governing privileged access also helps prevent risk from insider threats, identity compromise, and protects the infrastructure from malicious attacks and operator error. Additionally, this enables automation of access and authorization controls required for compliance standards such as NIST, GDPR, PCI, and HIPAA. Identity and Cloud Access Governance also provides audit and investigation teams access to valuable identity-related information including attributes, entitlements, access history, provisioning, role changes, and any other event related to the identity's access. One can further visualize and analyze this information using dashboards, graphs, and advanced reporting capabilities.

Cloud security is a journey, not a destination. The guidance offered by the NSA is a critical step in raising awareness and provides insight, so organizations know where to prioritize and optimize their security resources.

SailPoint helps protect high-value assets wherever they may exist across an organization's complex hybrid infrastructure – especially the cloud. SailPoint enables organizations to prevent malicious and accidental data exposure tighten privileged identity access, and stop insider and external cyber threats.

To learn more about how SailPoint can improve your cloud security, visit us at **www.sailpoint.com.**

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

EB1341-2002