SECURITY INNOVATION

7 SINS of Cloud Security

Over the last few years, our experts conducted hundreds of cloud application and infrastructure security assessments. While there are many techniques to combat threats, one of the biggest exposure points we saw was lack of (or improper use of) cloud-native services, such as secrets managers and alerting services.

Following are common mistakes organizations make that increase their cloud security risks:

1. **Failure to use Multi-Factor Authentication (MFA)** – this extra step makes it much more difficult for privileged accounts to become compromised and lead to complete account takeover.

2. **Improper IAM utilization** – broadly-scoped permissions can lead to overprivileged users or services, making for powerful pivot points in the event of a compromise. Take time to get familiar with Identity and Access Management (it's harder than you think!). Avoid wildcard access and reduce scope of permissions to specific business cases.

3. **Insufficient logging** – cloud providers have a wide range of logging and aggregation services available to aid investigation of security, development and configuration issues: access logging, network flow logs, API logging and others.

4. **Lack of alerting** – configure alerts to let your response team know when users or services are performing actions out of the ordinary. This could be higher than expected traffic load, multiple logins over a short period of time, or another anomalies.

5. **Improper secret/sensitive information storage** – encrypt sensitive data. Sounds obvious, but there's a lot to think about: identifying what is considered "sensitive", using sufficient cipher strengths, taking advantage of cloud provider secrets management services, and protecting your crypto keys.

6. **"Drag and Drop" migration** – migrating from on-premise to the cloud isn't simple. Setting up a firewall and segmenting your network are important, but there are other cloud-native services to think about: Secrets managers, alerting services, and IAM segmentation are paramount to ensure granular control of users and services. And applications aren't automatically more secure – many will need to be rewritten.

7. **Infrequent security reviews** – cloud environments increase in complexity quickly, so conduct regular audits of your cloud applications, accounts, and configurations. Pay particular attention to your IAM configuration and their storage. Also, take advantage of CSP security auditing tools that automatically flag misconfiguration and compliance issues including AWS Access Advisor, Azure Advisor and a host of others..

Cloud Security Checklist

In order to help your organization avoid these 7 Sins, we've provided this handy checklist to ensure your cloud systems are secure.

IDENTITY ACCESS MANAGEMENT

- [ ] Multi-factor authentication (MFA) is enabled for privileged accounts
- [ ] Users are segmented into roles and/or groups
- [ ] Permissions are granted to roles or groups rather than individual users
- [ ] Permissions are scoped tightly, avoiding the use of wildcard (*) access to actions and resources
- [ ] Cross-account access configuration is scoped to specific use cases
- [ ] Access keys are rotated on a regular basis
- [ ] Users with multiple keypairs are flagged for business use case review

COMPUTING

- [ ] Only standard and expected access methods are enabled for computing resources
- [ ] Prefer keypair authentication over password authentication where possible
- [ ] Build packages are up-to-date with the latest security fixes
- [ ] Computing resources are segmented by logical security groups
- [ ] Security groups properly restrict inbound/outbound network traffic to specific use cases
- [ ] Virtual machine instance storage encrypted at rest, either via disk or file system encryption

DATABASES

- [ ] Sensitive data is encrypted
- [ ] Backups are enabled
- [ ] Availability zones are defined to meet business availability needs
- [ ] Backups and/or snapshots are not publicly available
- [ ] Retention periods are sufficiently long

OPERATIONAL

- [ ] Billing alerts are set up to catch excessive usage early
- [ ] Security contact is defined
- [ ] Security contact information is up-to-date
- [ ] Account configuration is reviewed from a security standpoint on a regular basis

LOGGING & MONITORING

- [ ] Relevant services have API logging enabled
- [ ] Alerting rules are configured to notify teams of potential threats, including events like high network traffic, sensitive actions such as disabling logging, and high load on computing resources

NETWORKING

- [ ] Logical virtual subnets are in place to segment resources appropriately (e.g., production vs test)
- [ ] Services are configured to use TLS 1.2 or newer
- [ ] Network security groups are configured to restrict inbound/outbound traffic to only required ports necessary to function

STORAGE

- [ ] Sensitive data is encrypted at rest
- [ ] All data is encrypted in transit
- [ ] Critical files are versioned or otherwise backed up
- [ ] Private files are not publicly accessible
- [ ] Storage is not world-writeable or world-listable
- [ ] Access to critical data is logged

Get in **Touch** | 187 Ballardvale Road, suite A195
Wilmington, MA 01887
887.839.7598 x1
www.securityinnovation.com