CLOUD SECURITY TESTING

How do you know you're covered?

The cloud has become a valued part of modern infrastructure and there are now more resources than ever to help organizations secure their cloud environments. Even with all of the available tools and resources, there are still a million ways to configure services incorrectly. Public and non-public breaches seem to happen weekly and the maturity of the information security program doesn't seem to influence the likelihood of the breach. One easy mistake in a cloud environment can be disastrous and it's reasonable to be concerned when a new breach report hits the news.

After the recent CapitalOne breach, we've had numerous concerned clients reach out to ask if they're going to become the next headline. While the details of the actual breach have trickled out in bits and pieces, at a minimum, we simply know that there were misconfigurations in their cloud that led to access to sensitive data that was stored in S3 buckets. Many of the technologies that were in use in CapitalOne's environment are in use in everyday environments, so it's no surprise that people are concerned about becoming the next breach.

Just like anything in security, there are no magic bullets, but to help address these concerns, NetSPI recommends some general guidelines to help get ahead of the cloud security curve. These are general best practices that could be applied to any portion of your IT environment, but it's good to keep these in mind while working with the cloud.

Practice Proper Cloud Hygiene

1. DEFINE REQUIREMENTS

- Starting with a solid understanding of the environmental requirements will help minimize your cloud services bills and your attack surface areas.

2. ISOLATE YOUR DEV/STAGE/PROD ENVIRONMENTS

- This is typically standard practice for development environments, but we have seen countless environments that started as a dev environment and eventually morphed into the production environment.
- Test applications, extra services, and other experiments that come up as part of the development process can all increase the likelihood of a compromise in the cloud. Limit your exposure by keeping these risks locked into your separate dev environments.
- Create a production account/subscription that only gets the final version of the code/deployment/etc. and keep that environment locked down.

3. LIMITED PRIVILEGES IN ALL ENVIRONMENTS

- Excessive privileges in that separate development environment may allow an attacker to escalate up to an account with full control over your cloud provider account. Keep those permissions in check and think about keeping fully separate accounts for dev and prod environments.

Test Regularly and Fully

1. PENETRATION TEST ALL THE LAYERS OF YOUR ENVIRONMENT

- While your application may be the entire reason for your cloud presence, are you looking beyond the application layer? What issues might exist in your WAF, or the VPN used to remotely administrate the virtual machines? By looking at the full spectrum (all IPs, hostnames, etc.) of cloud services that are in use in your environment, you can obtain better coverage of potential soft spots.

2. UTILIZE CLOUD CONFIGURATION REVIEWS

- Many organizations are just looking at the network and application layers for their cloud environments. Traditional penetration testing against cloud environments can be helpful, but it doesn't cover all of the cloud bases. With standard external testing methods, we can only see what we can see, so additional issues can exist under the surface. With access to the cloud environment with a configuration account, your testing team can find potential exposures that would not normally be exposed through traditional penetration testing methods.
- You don't need to give away the keys to your cloud kingdom, but a read-only account in your cloud provider could be the difference in identifying hidden issues in your cloud deployment or missing major issues that could lead to a breach.

	EXTERNAL PENTEST DELIVERABLES	CLOUD PENTEST DELIVERABLES
Perform live system and service enumeration	X	X
Perform information gathering	X	X
Perform open source intelligence gathering	X	X
Perform automated and manual vulnerability enumeration	X	X
Identify non-public data exposure without authentication	X	X
Identify code, configuration and patch related vulnerabilities within exposed operating system services, applications and cloud components using manual and automated processes	X	X
Identify single factor management interfaces	X	X
Evaluate test results and identify false positives	X	X
Perform exploitation of identified vulnerabilities Attempt to pivot into in scope networks	X	X
Testing on cloud hosts and services	POTENTIAL	X
Network Penetration Testing will include internal network layer testing of virtual machines and services from the cloud virtual networks & external network layer testing of externally exposed services		X
Configuration review of Cloud Services: review of firewall rules, IAM/RBAC review of users/roles/groups/policies, review of utilized Cloud Services (including, but not limited to, Storage, Databases, Serverless Computing, etc.)		X
Expert configuration review of cloud platform and infrastructure services		X

If you're interested in assessing your cloud environment, reach out to the NetSPI team at sales@netspi.com. We're always happy to answer questions to help you find the right ways to help you secure your cloud.