SERVICE DESCRIPTION

SpiderLabs Amazon Web Services (AWS)

Service Scope

Amazon Web Services (AWS) is a collection of cloud computing systems provided by Amazon. It provides software-as-a-service, platform-as-a-service, and infrastructure-as-a-service (IAAS) options.

This security assessment actively validates the adherence to security policy and lists specific remediation items for each problem identified. The test is typically conducted in the following manner but is tailored to specific requirements.

Scope and Project Phases

In our AWS assessment, the SpiderLabs consultant will assess the configuration and security of an Amazon Web Services setup. This is performed in both and automated and manual manner, utilizing various custom tools. The assessment includes, but is not limited to, the following areas:

- Identity and Access Management (IAM) Configuration and hardening:
  - Access keys and root account status
  - User groups and privileges
  - Password policy
  - Multi-Factor Authentication (MFA) configuration
  - IAM roles for EC2 instances
- CloudTrail
- S3 Bucket Security
- IDS / IPS analysis, if appropriate
- Policy configuration
- Tenancy mode
- Encryption of snapshots and volumes
- Use of zones / Virtual Private Clouds (VPC)
- Region in which data is held

- Outbound EC2 access restrictions
- Protective Monitoring (detection and response) including Amazon GuardDuty
- Security groups configuration and setup, and access limitations

Scope exclusions

- This assessment will not include any review of the sizing and/or optimization of the environment
- This assessment will not include any configuration changes / optimization for Denial of Service (DoS) protection

Customer Requirements

- The customer will provide credentials and/or access to the environment(s) required to perform this assessment.
- If appropriate, the customer will obtain necessary approvals from the hosting provider in order to authorize this assessment.
- To perform a full audit, both the Access Key ID and Secret Access Key should be supplied.
- The customer will ensure there is a dedicated point of contact with the necessary knowledge and authority to progress any queries and/or escalations from SpiderLabs.

Deliverables and Outputs

Following the conclusion of the engagement, findings will be made available via the TrustKeeper Portal. The issues disclosed will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.