SERVICE DESCRIPTION

SpiderLabs Azure Cloud Assessment

Service Scope

Microsoft Azure is a cloud computing system provided by Microsoft. It provides software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) options.

This security assessment actively validates adherence to security policies and describes specific remediation advice for each security issue identified. The test is conducted in the following manner but is tailored to specific requirements.

Scope and Project Phases

In an Azure assessment, Trustwave SpiderLabs' consultants assess the configuration and security of a Microsoft Azure IaaS system. This is performed in both an automated and manual manner, utilizing various custom tools. The assessment includes, but is not limited to, the following areas:

- Active Directory and administrator accounts, and password policy (if aligned to existing AD policies)
- Granularity of Azure administrator auditing configuration
- User groups and privileges
- Authentication mechanism used (SAML 2.0, OpenID Connect, OAuth2, WS-Federation) and any associated weaknesses
- VNET configuration – use of RFC1918 addressing and subnetting
- Security context of services running
- ExpressRoute configuration (if applicable)
- The virtual machines deployed, their build and secure configuration
- Endpoints configured and network filtering or controls, such as RDP, applied to protect access to them
- Service Bus Queue configuration
- Proxy connector – how transport security is configured and how the underlying VM is secured (from a build perspective)
- Data at rest options on VMs (such as any disk or file encryption capabilities)
- Anti-virus or anti-malware capabilities
- Data exfiltration

- Protective monitoring and logging (Monitoring APP registrations Azure AD logging)

In order to complete the assessment in a reasonable time, SpiderLabs will require:

- All necessary change requests raised and approved for the nominated consultant(s) on the requested testing dates to enable access for testing.
- A co-admin (typically a global admin) account for the Azure Management Portal, configured for access to the client Azure instances.
- If appropriate, access to the Secure Score portal, to ensure best practice is enabled across the infrastructure.

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.
- 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.