Service Definition
Cloud Security Assessment

Introduction

NTA's Cloud Security Assessment allows organisations who are using cloud hosted software, infrastructure or platforms, to gain independent analysis and information security assurance regarding the governance and controls that are in place to protect these services and systems. Such assurance is vital for cloud based services which possess specific security considerations due to their on-demand, remotely accessible and multi-tenanted attributes.

All security issues found are detailed in a formal report and recommendations are provided to enable the customer to eliminate or mitigate the risk, thus greatly reducing the likelihood of a successful attack.

This specialist testing service provides customers with governance support when migrating to or integrating with cloud based services.

Scoping

A scoping conversation will be held prior to delivery to fully understand requirements and expectations, the size of the platform/environment to be tested and the type of systems and/or infrastructure to be assessed. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

With the ever-increasing use of cloud hosted software, infrastructure or platforms, testing of these deployments provides an independent analysis and information security assurance regarding the governance and controls that are in place to protect services and systems. Such assurance is vital for cloud-based services which possess specific security considerations due to their on-demand, remotely accessible and multi-tenanted attributes.

The range of activities performed vary from ensuring appropriate separation controls between tenant environments to full reviews of the platform using the CSA CCM (Cloud Security Alliance, Cloud Control Matrix) to evaluate the security services offered by the Cloud Service Provider (CSP).

The service can be tailored to suit individual assurance requirements, focusing on Internet-facing services or applications only or the backend infrastructure that supports these also.

Areas covered include, but are not limited to, the following:

- Testing of Internet-facing network services for operating system, configuration and software vulnerabilities
- Testing of cloud hosted applications for vulnerabilities using industry standard frameworks, e.g. OWASP Top Ten
- Testing of underlying virtual servers and infrastructure to ensure that it is not possible for an internal attacker (or an external attacker who has gained access to the internal infrastructure) to compromise the environment and gain unauthorised access to system functions, resources or data; or for an authorised user to manipulate or exploit the system to gain unauthorised access to non-permitted system functions or resources. Areas covered typically include some or all of the following:
    - Cloud service components and technologies (e.g. Route53, CloudTrail, Lambda, EC2 instances, S3 buckets, Azure Blobs etc.)

  - Virtualisation and Containers (e.g. Docker, Kubernetes)
  - Security Groups and Network Access Control Lists (NACLs)
  - Identity and Access Management (IAM) and Active Directory Roles
  - Center for Internet Security (CIS) benchmarking (e.g. server/database configuration)
- Testing of remote access services (e.g. configuration and security of Administrator portals; insufficient policies, RBAC, networking and/or logging)
- Review of network topology (e.g. gateways, routes, tenant segregation, etc.)
- Review of Cloud logging solutions (e.g. CloudWatch, Azure Monitor)
- Configuration reviews of VPC's to ensure sensitive information is not publicly exposed, and that the Cloud environment complies with industry best practice standards

Deliverables

The output is a tailor-written formal report containing:

- An executive overview with business implications
- A summary of risks identified, ordered from high to low severity
- Technical details of each issue found
- Recommendations for closing holes found
- Full listing of test results tables including background information/evidence to support results

The style and format of the report is designed with clarity and ease of use in mind. Features include hyperlinks to relevant sections of the document as well as external sources where applicable.

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the testing and the key findings and potential business implication (severity) of the issues found. This will include suggested priorities for the customer to take action against.

Service Management

You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Service Definition
Cloud Security Assessment

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities
The customer is responsible for the completion of a Technical Details Form (TDF) prior to delivery. The provision of appropriate information will ensure that delivery meets expectations and requirements.

Technical Requirements
The resources typically required from the customer to ensure the service is performed as efficiently as possible include:

- For Internet-facing Cloud services or applications:
  - Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
  - A list of target Internet IP addresses
  - Details of all Fully Qualified Domain Names (FQDNs) and any other unique entryways into applications, remote access or other systems for the entire in-scope infrastructure

- For underlying virtual servers and infrastructure:
  - Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
  - Where physical access to the target environment is not possible:
    - Provision of a suitable VPN connection from NTA's office
    - Pre-configured 'virtual test machines' provided by NTA installed within the target environment (full support and details for successful implementation available)
    - Provision of relevant documentation for review as appropriate (e.g. network diagram, firewall configurations, etc.)