Service Definition
Remote & Mobile Access Security Assessment

Introduction

With the increasing pressure for staff to be able to remotely access data held within the cloud or corporate network, the need to finely balance access with security and ensure appropriate governance controls is perhaps at its greatest.

NTA's Remote & Mobile Access Security Assessment provides an examination of remote access systems, mail gateways and Mobile Device Management (MDM) solutions, testing for operating system and software vulnerabilities as well as vulnerabilities within the configuration of the portals and authentication mechanisms.

This service allows organisations who have procured services via the Digital Marketplace, or 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.

This specialist testing service provides customers with governance support in relation to the integration of cloud based services and systems into their organisations.

Scoping

A scoping conversation will be held prior to delivery to fully understand requirements and expectations, the type of remote & mobile access solutions deployed and to discuss any particular concerns. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

This service may be purchased either individually or as a collection of services offered by NTA Monitor.

The approach to service delivery may vary depending on the solution used, as follows:

- ***SSL VPN & Citrix Secure Gateway***
  SSL and Citrix remote access servers present little opportunity for remote compromise by unauthorised users, as they generally only offer one port and one log-on screen to the Internet. Testing would seek to ensure that this is the case and would check that the authentication process is sound, that appropriate encryption is in place and that the system is not vulnerable. For authenticated testing, NTA would look to identify vulnerabilities that would allow a user to sniff traffic, map the drives, change the configuration settings of the system or break out of permissible applications into other areas of the network.

- ***IPsec***
  Testing of an IPsec VPN solution would seek to determine as much information as possible about the configuration and security of the target VPN Server and to establish if it is possible to gain access to the network through this device. The VPN Client can also be tested to assess the threat presented to the internal network by a normal remote user and by someone who has stolen or gained unauthorised access to a client.

Service Definition
Remote & Mobile Access Security Assessment

- ***Site-to-Site VPN***
  NTA would test the VPN server IP address for vulnerabilities that may allow access to the corporate network. This should prove that, in its current configuration, the VPN is not externally visible and is secure.

- ***Webmail***
  The webmail solution used (e.g. OWA) would be tested for vulnerabilities that that may allow an unauthorised user to access internal mail records, monitor mail traffic or perform a Denial of Service attack against the mail system. For authenticated testing, NTA would check for known vulnerabilities within the product and will also check that it has been configured securely.

- ***Mobile Device Management (MDM)***
  Testing would focus on two aspects of the MDM service deployed; The first is the external communication of the application with the server where NTA will attempt to intercept and manipulate the traffic to enable an attack or information disclosure; The second is the enrolment process where attempts will be made to trick the process into accepting dangerous situations (e.g. allowing us to enrol a malicious device). It is recommended this activity be supplemented by a security assessment of a mobile device with the MDM software installed, which is delivered as a separate service.

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
- Recommendations for closing holes found
- Technical details of each issue 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 assessment 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.

Service Definition
Remote & Mobile Access Security Assessment

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.

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:

1. Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
2. VPN server IP address/URL for the Log On Screen
3. User credentials for two sets of user accounts (where applicable)
4. Additional authentication requirements (e.g. RSA tokens, client certificates, version or software details)