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.

Intertek NTA's Remote & Mobile Access Test 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. 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.

Intertek NTA frequently identify vulnerabilities that could allow attackers to take control of a server, access the internal network, interrupt connectivity or gain unauthorised access to corporate or other user's sensitive data. If such events were to arise, the cost to the organisation could include loss, corruption, disclosure or ransom with intent of extorsion of data, the inability to support remote workers, a damaged reputation and the man hours required to get systems up and running again.

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 Intertek NTA.

Given the high volume of tests that are performed, Intertek NTA is familiar with testing a wide variety of system and software types. Examples of specific vulnerabilities found by the service include:

- Users can 'break out' of published applications and virtual desktops/environments
- Internet access on the remote host/server running Remote Desktop for data exfiltration
- Windows user accounts can be enumerated via various methods
- Potentially sensitive shares can be viewed on pooled server
- Cisco ASA Appliance WebVPN cross site scripting vulnerability
- Static session ID is used before and after authentication
- Windows command prompt can be executed to further privilege escalate
- MS Exchange OWA server not up-to-date with latest update rollups
- Citrix server user address book can be enumerated by authenticated user

Examples of generalised findings include:

- Local privilege escalation due to weak configuration of services or applications as well as operating system and application vulnerabilities

- Searching the local filesystem for sensitive information or passwords in files which could lead to systems being compromised on the network
- Passive network sniffing to enumerate the environment and potentially capture sensitive information
- Accessing the remote access system using unenrolled devices

Test Approach

SSL VPN & Citrix Secure Gateway
This test would consist of both a pre- and post-authentication element:

1. ***Unauthenticated Perspective***
   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. This stage of testing would seek to ensure that this is the case and would check that the authentication process is technically sound, that appropriate encryption is in place and that the system is not vulnerable due to poor configuration, data sanitisation or brute force attacks etc...

2. ***Authenticated Perspective***
   It is recommended that authenticated testing of the remote access system be conducted. Intertek NTA would look to identify vulnerabilities that would allow a user to find local files containing known passwords or configurations that allow privilege escalation attempts, map local drives for data exfiltration, change the configuration settings of the system or break out of permissible applications into other areas of the network/environment. This element of testing includes a limited security analysis of the applications and utilities that can be accessed. From this perspective it is also possible to properly test the authentication process as this is 'exercised'.

If present, two factor authentication controls would also be tested.

IPsec VPN
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.

Web Mail (OWA etc)
This test would consist of both a pre- and post-authentication element:

1. ***Unauthenticated Perspective***
   Intertek NTA's Web Mail Security Test examines the Outlook Web Access and similar systems 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.

2. ***Authenticated Perspective***
   Intertek NTA will check for known vulnerabilities within the product and will also check that it has been configured securely. An examination of Active Sync and OWA will be performed if these facilities are offered.

Mobile Device Management (MDM)
Testing would focus on two aspects of the MDM service deployed; The first is the overall configuration and application of the policies applied to the corporate devices from the on prem or cloud based MDM solution; The second is the a review of the configured policies in line with best practice guidance available at the time of testing. It is recommended this activity be supplemented by a security assessment of a mobile device with the MDM software/policies installed and applied, which is delivered as a separate service.

The service is engineered to ensure that no damage is caused. Limited exploitation is performed to prove exploits such as cross-site scripting, but with damaging exploits and denial of service attacks not being performed. Options are available for more exploitative testing should this be required.

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.

Intertek 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, Intertek 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 Intertek 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)