Service Definition
PCI ASV Scanning

Introduction

Intertek NTA's PCI ASV Scan is designed to fully meet the requirement for external quarterly network vulnerability scanning as defined by point 11.3.2 of the Payment Card Industry (PCI) Data Security Standard (DSS).

Extract from the PCI DSS:

11.3.2 "External vulnerability scans are performed as follows:

- **At least once every three months.**
- **By a PCI SSC Approved Scanning Vendor (ASV).**
- **Vulnerabilities resolved and ASV Program Guide requirements are for a passing scan are met.**
- **Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan."**

Intertek NTA has been an Approved Scanning Vendor (ASV) for over 19 years and our current ASV certificate number is 4183-01-19. The test, process and report provided by this service are in line with the ASV Program Guide v4.0 r22, with Intertek NTA being examined annually in order to confirm adherence to these standards.

Intertek NTA has delivered this service to a number of government, financial, retail and service sector organisations since 2006, and is approved for delivery to UK and global clients.

Scoping

To provide a cost for the service Intertek NTA would need to know how many live/active IP addresses there are in scope for testing.

Service Overview

Intertek NTA frequently identify vulnerabilities that could allow attackers to deface a web site, take control of a server, access the internal network, interrupt Internet 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 or disclosure of data, the inability to send or receive email, a damaged reputation and the man hours required to get systems up and running again.

If any high or medium risk vulnerabilities are found, the scan report will be marked as a fail and the client will be non-compliant with PCI DSS standards. Therefore, to support the client through this critical process, Intertek NTA provides immediate notification of any such fail vulnerabilities along with a recommendation on how these may be fixed. If such issues are subsequently fixed, Intertek NTA will provide a free-of-charge single spot retest of these fail issues to ensure they have been closed effectively and reissue the test report to confirm the current and improved state of security. The retest must be within two weeks of initial report provision.

The PCI ASV Scan checks for network and unauthenticated application level vulnerabilities on all systems within the target IP range that are visible from the Internet. 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 fail vulnerabilities found by the service include:

Service Definition
PCI ASV Scanning

- Web application has cross-site scripting vulnerability
- Web server has cross site tracing vulnerability
- Web servers support unencrypted HTML form based authentication
- SSL version 2 supported
- Internet servers allow Windows Terminal Server access
- Database connection string disclosed
- Directory Listing available through PROPFIND method
- VPN server supports IKE Aggressive Mode
- Microsoft Outlook Web Access URL redirection
- Unsupported operating system detected
- Exposed CMS admin interface

Test Approach

Intertek NTA would conduct network probing to identify all systems visible from the Internet within the specified IP address range, including routers, firewalls, web application, remote access systems, mail and domain name servers. Where found, these systems will be tested for vulnerabilities within the operating system, the software and their configuration.

Unauthenticated application level testing would also be conducted against any web-based applications, remote access or file transfer systems found within the specified IP range, to identify flaws such as insecure authentication, weak encryption, SQL injection, faulty lockout facilities and cross-site scripting.

In line with the PCI ASV Program Guide, tests will identify vulnerabilities in the following key areas:

Firewalls and Routers	Web Applications
Operating Systems	Other Applications
Database Servers	Common Services
Web Servers	Wireless Access Points (if Internet visible)
Applications Servers	Backdoors
Common Web Scripts	SSL/TLS
Built-in Accounts	Remote Access
DNS Servers	POS Software (if Internet visible)
Mail Servers	Port/Service Discovery and Fingerprinting

The service utilises Intertek NTA's unique test software, which is self-scripted and maintained in-house, along with selected open source and commercials tools where appropriate. This provides the benefit of our test engineers fully understanding the inner workings of the test engine and thus understanding how the results are derived, greatly increasing the accuracy of the service.

A test engineer would assess and correlate the findings of the initial automated stage and perform manual verification and further testing of any results that look unusual, any systems that appear to be complex or offering multiple ports, or systems for which there are conflicting results.

Service Definition
PCI ASV Scanning

The service is engineered to ensure that no damage is caused to networks. Damaging exploits and denial of service attacks are not performed.

Deliverables
A formal report following the guidelines outlined by PCI is provided, containing:

- Statement of PCI Compliance (Pass or Fail)
- A summary of risks identified, ordered from high to low severity
- Technical details of each issue found
- Recommendations for closing holes found

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 such as patch updates, recommendations and CVE/CVSS references.

Additional support is provided in the form of an optional telephone technical debrief plus free of charge retesting of any fail issues identified.

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.

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 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 such as target IPs and URLs will ensure that delivery meets expectations and requirements.

Technical Requirements
1. Technical contact details for any necessary communication during the scanning (e.g. high risk issue notifications)
2. Target Internet IP addresses (ranges or single IPs) to be included in the scan

3. List of Fully Qualified Domain Names (FQDNs) or any other unique entryways into applications for the in-scope infrastructure
4. Details or any load balancers used