Service Definition
NCSC CHECK IT Health Check

Introduction

G-Cloud customers and Government authorities/departments who are implementing new infrastructure or applications, particularly when the processing or storage of data associated with that environment is marked OFFICIAL-SENSITIVE or above under the Government Security Classification scheme, will require a National Cyber Security Centre (NCSC) CHECK standard IT Health Check of the new service and usually annually thereafter. The IT Health Check will often also support Risk Management Accreditation Document Set (RMADS), Government Accreditation activities and annual compliance requirements.

A NCSC CHECK standard IT Health Check is conducted by an independent third party that is accredited by NCSC. Intertek NTA (NTA) has been a NCSC CHECK certified provider continuously since 1999 and has extensive experience of providing IT Security Health Checks for local and central Government authorities, Police and NHS organisations, as well as Critical National Infrastructure (e.g. SCADA) environments.

Scoping

A scoping conversation will be required at the outset of the engagement to ensure the requirements are aligned with associated RMADS, Accreditation or compliance activities and principle security concerns are sufficiently considered/included within the service proposed. 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.

NTA conduct this service in accordance with the terms and conditions of the NCSC CHECK standard, with delivery performed by CHECK (Team Leader and Team Member) approved consultants. Each engagement is dependent on the environment to be assessed and list of Targets of Interest (ToI) or Principle Security Concerns (PSCs) but will broadly include some or all of the following, where applicable:

- External Network Assessment
- Internal Network Assessment
- Cloud Infrastructure & Services Assessment
- Web Application Testing (including APIs/web services and/or mobile as applicable)
- Server Build Review
- Database Configuration Review
- Firewall Configuration & Ruleset Review
- Client/Mobile Device Lockdown Assessment
- Wireless Network Assessment

Deliverables

The results presented will be categorised by risk and will follow the requirements outlined by NCSC for providing a formal report. A clear explanation of each vulnerability, the rating applied (High, Medium and Low), justification of how this rating has been reached and recommendations to enable the vulnerability to be mitigated will be provided.

Service Definition
NCSC CHECK IT Health Check

The report will also consider the sum of all issues and advise on an overall risk rating, given that a series of lower risk vulnerabilities may combine to present a higher threat. The report will include hyperlinks, both for navigation within the report and to access external resources such as CVE details at the NVD website, CVSS score referencing where possible, patches at the Microsoft website etc.

The report will contain:

- 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
- Screen shots and supporting evidence for risks found

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the IT Health Check 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 and allows for the specific environment to be considered and the actual business and operational impact to be refined.

NTA has a formal process for managing false positives and other disputes that arise following presentation of the report. This allows NTA to give due consideration to the appropriateness of the rating and acts as mechanism to ensure that ratings are justified and applicable to a specific environment.

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 security classification of the contents.

Information Assurance
NTA is security cleared to perform information security testing services on infrastructure, platforms or software with a Government Security Classification up to SECRET.

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.

Service Definition
NCSC CHECK IT Health Check

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 internal activities at the customer's location, typically:
1. Accessibility to all infrastructure, applications and components in scope of testing
2. At each test point the tester(s) will require: 2x physical ports, 4x IP addresses per VLAN and/or 2x physical ports, 4 x IP addresses per LAN
3. Availability of switch point, switch name, switch location and IP address(es) the tester(s) will be plugging into to perform testing
4. Application support, where applicable, for the testers during delivery
5. Test accounts (login/authentication details) and the assigned user roles for application(s) in scope
6. Someone available onsite who can give us access to the network for testing purposes (i.e. a System Administrator or Network Manager). The designated contact should also be able to provide any necessary documentation (e.g. relevant network topology diagrams, firewall rule bases in electronic format (preferably .xls), administrator level credentials, etc.)
7. Power supply, table and chairs for the tester(s)

For external testing activities, typically:
1. A list of target Internet IP addresses
2. 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