Service Definition
IP Telephony (VoIP) Security Assessment

Introduction

NTA's IP Telephony (VoIP) Security Assessment service provides a review of the configuration of the IP telephony system to determine if the corporate voice and data networks are exposed to security threats.

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 purchase of the service in order to fully understand the setup and features of the technology being used and to discuss any particular areas of concern. 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.

IP Telephony (or VoIP) is a popular choice because of the efficiency and cost savings that it offers. However, simply replacing one technology with another does not remove the risks posed; it just introduces a different set that must be guarded against.

The service involves analysing and reviewing the IP telephony design, system configuration, network topology and security procedures in place, as well as any other security related management and administrative aspects. These will all be compared against good governance and best practice, with any areas that don't follow such guidelines being highlighted.

The servers that provide call set-up and/or routing will be assessed, as well as the firewalls that pass the VoIP traffic.

Specific vulnerability examples include:

- Usage of mac address filtering
- Ability to redirect/monitor calls
- Administrator level penetration on VoIP windows/unix call management servers
- Caller ID spoofing
- VLAN hopping attacks
- SIP – to see whether it is possible to intercept SIP requests and change them (and thereby alter call routing) through the capturing of RPT requests
- Use of poor encryption or integration controls on H323/H225 protocols

- 'Peripheral' or 'Management' boxes having been attached to the telephone system
- Usage of encryption
- Wireless VoIP elements

Testing will start with packet interception for phone booting and making/receiving calls to determine what protocols etc. are being used. The test then moves on to network/switching attacks and VLAN attacks, assuming the voice and data VLANs are separated, followed by attempts to map the parts of the system that are accessible from the telephones/desktop PCs and testing these visible areas for further potential vulnerabilities.

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 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.

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
IP Telephony (VoIP) 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. The customer is also responsible for providing physical and logical access to all areas in scope, e.g. point of contact at the site location to be tested, network access and valid user credentials.

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

1. 2 x CAT5 ports and 2 x telephones connected to the system with their network ports set up as normal
2. A network diagram of the telephony network to evaluate and confirm the systems in scope of testing