Service Definition
Physical Security & Social Engineering

Introduction

Regardless of the time and money spent on protecting a network with the latest security technology, it is the security processes of an organisation that can often be the weakest link in securing information. Using an independent social engineering service is the most effective way of testing the human, physical and procedural defences within an organisation.

Intertek NTA's Physical Security & Social Engineering service determines what vulnerabilities exist, such as weak staff security awareness, physical controls or procedural controls that may allow unauthorised access to corporate information, either directly or via the IT systems that hold this data.

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, site locations and departmental areas to be assessed (incl. hot spots and no-go areas/staff) 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 Intertek NTA.

The service focuses on identifying weaknesses through interaction with the social, physical and procedural aspects of the organisation.

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.

The service is split into two phases – 'Remote/Off Location' and 'Physical/On Location'. Within each phase there are a number of modules, allowing for a suitable service to be tailored.

Remote/Off Location

- Review of online social media/blog sites to gather sensitive data or information to aid the next stage of attack
- Attempt to obtain username and password to a valid user account by telephone from the IT helpdesk or from general staff by masquerading as the helpdesk
- E-mail and telephone attempts to extract sensitive/confidential information from a cross section of staff

Service Definition
Physical Security & Social Engineering

- Construction of a fake web portal, masquerading as a site belonging to the organisation, with selected staff being encouraged, via a phishing email, to visit this site and disclose confidential information

Physical/On Location

- Attempt to bypass physical access controls into any office or building, providing photographic evidence of entry
- Work unchallenged from a vacant staff desk, obtaining network access if possible
- Gain access and work unsupervised for five minutes in a server room or other secure area
- Covertly observe or provide agreed audit of adherence to best practice information security controls such as clear desk policy, locked workstations etc.

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
- Details of each issue found
- Recommendations for closing holes found
- Photos and other supporting evidence for risks found

The style and format of the report is designed with clarity and ease of use in mind.

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.

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

This service has elements that involve Intertek NTA's consultant(s) attempting to gain 'perceived' unauthorised physical access to buildings and offices. Therefore, it is the customer's responsibility to ensure that in the event that a consultant is successfully challenged they are able to demonstrate (via both a valid letter of authority and personnel contact details for the duration of the exercise) good reason for their activities.