SERVICE DESCRIPTION

SpiderLabs Social Engineering & Phishing Testing

Service Scope

The Trustwave SpiderLabs Social Engineering & Phishing Testing service results in an in-depth test of the entire target workforce and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target workforce. These recommendations are both actionable and advisory in nature and are presented to the customer.

The service methodology ensures that the test methodically, iteratively and quantitatively assesses the human factor of security by determining the susceptibility of the target workforce to social engineering and phishing attacks.

Social engineering is the act of manipulating people into performing actions or divulging confidential information. This attack can occur over varying mediums, including but not limited to, email, phone as well as face to face.

The primary objective of this security test is to determine an employee workforce's resiliency to the common attack vector of social engineering attacks. Increasingly, as organizations harden their perimeter and add security systems to keep intruders out, direct attacks against the perimeter network become more difficult to carry out, leaving the targeting of individual employees an attractive prospect for attackers intent on gaining unauthorized access to an organization.

Scope and Project Phases

In executing this test, Trustwave will use methods simulating those of an external attacker, but within a controlled manner to profile, target and ultimately gain unauthorized access to the target organization.

Organizational Intelligence

Trustwave will perform research using Internet source and various public databases to compile a catalogue of information about each corporate location and facility to be considered in scope for the test. This information typically includes but is not limited to:

- Information of employees at location (via social networks)
- Information about events occurring in or around facility

Copyright © 2018 Trustwave Holdings, Inc. All rights reserved.

- Business partners
- Information on Executive staff
- IT infrastructure

This information is then collated to create several plausible scenarios that will give Trustwave consultants several possible approaches to gain unauthorized access to sensitive information, accounts, and facilities.

Attack Simulation

Once the organizational targets have been verified, Trustwave will execute the attack simulation phase. This phase consists of exploit delivery through forged emails, phone calls, onsite personal interaction onsite, and other delivery methods. Scenarios can involve, but is not limited to, Trustwave consultants impersonating:

- Employees, consultants, or vendor representatives
- Delivery or courier staff
- A lost tourist, guest, or customer
- Construction workers
- Executive staff
- Candidate for a new job
- Security guard or staff

Data Extraction

Should Trustwave have success during the attack phase, Trustwave consultants will securely maintain the compromised data and other assets until the end of the test. The focus of this portion of testing will be unauthorized access to sensitive data such as corporate internal information, PII, or CHD. This allows for better assessment and appreciation of the impact and associated with each attack vector.

Deliverables

Following the conclusion of the engagement, findings will be made available. The deliverables will be both strategic and tactical in nature, presented in a format that is highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.

Copyright © 2018 Trustwave Holdings, Inc. All rights reserved.