CYLANCE CONSULTING

Social Engineering Assessment

Improve Security Defenses through "People Hacking"

Benefits

- Determine readiness in detecting and eliminating potential social engineering threats
- Test established security controls and procedures
- Understand real-world risks from the perspective of an attacker
- Measure the effectiveness of security awareness training

30% of phishing messages were opened by the target across all campaigns and about 12% went on to click the malicious attachment or link enabling the attack to succeed.

Source: Verizon Data Breach Investigations Report 2016

Employees represent a potential weak link in security for many organizations. While employees don't have to be malicious to put the organization at risk, they may not understand the security risks associated with their behavior and their role in protecting critical business information.

Social Engineering Assessments help organizations **understand the real-world threats** to their business from the view of an attacker. Social Engineers attempt to gain access to protected information by exploiting unsuspecting staff members. These assessments help **identify the potential holes in the "human element"** to **prevent information breaches** and to **strengthen the company's security and compliance posture.**

Service Overview

Cylance® Consulting's Social Engineering Assessment attempts to convince the organization's employees to divulge sensitive information through pre-defined test scenarios. The assessment can help establish the current state of security awareness among employees as well as determine gaps in policy, procedures and enforcement.

An assessment is performed in a variety of ways:

- **Open Source Intelligence (OSINT) Gathering —** Attempts to uncover as much information about the organization as possible from publicly available data
- **Phishing Attacks —** Carefully crafted emails are sent to selected employees with the goal of convincing them to visit a "malicious" website through a link or downloading "malicious" documents
- **USB Stick Drops —** USB sticks are left throughout the campus with a "malicious" document aimed at enticing an employee to open it
- **Phone-Based Social Engineering —** Selected employees receive phone calls asking them to provide their network login credentials and other sensitive information

Deliverables

Cylance Consulting will furnish a comprehensive report detailing:

- Descriptions of the attack vectors employed
- Which vectors were successful/not successful with particular employees

We can also work with your team to help design security awareness training focused on thwarting social engineering attacks.

Improve your security defenses through social engineering assessments. Contact Cylance Consulting or your technology provider for details.

CYLANCE

+1-877-97DEFEND
proservices@cylance.com
www.cylance.com/consulting
18201 Von Karman Avenue
Suite 700, Irvine, CA 92612