Social Engineering Testing Service
Uncover the weakest link in the security chain

Despite organizations have matured their defense mechanisms to protect against sophisticated security attacks, deploying advanced protections and monitoring controls including vulnerability scans and penetration tests, still serious security breaches are commonplace and sensitive organization information are getting disclosed.

Social Engineering is generally agreed upon as the weakest link in the security chain. Many of the most damaging security violations are due to employee security breaches and the use of Social Engineering attacks.

As Social Engineering attacks are described the non-technical intrusions into a business environments that rely on human interaction, often involving tricking people in order to break normal security policies.

Most commonly, as part of targeted Social Engineering attacks, on a daily bases phishing emails are likely to be reaching your employees' inboxes and, it's a matter of time when someone within your organization will click, or reply therefore exposing your organization's network and confidential information. Based on recent report[i] from TrendMicro, spear phishing attacks continue to be a favored means by APT attackers to infiltrate target networks.

- Protect your organization against emerging threats.
- Reduce the risk from targeted phishing and malware attacks.
- Determine the effectiveness of your security awareness training.
- Determine how vulnerable your users' web browsers are to the exploits that attackers are using today.
- Increase your employees' knowledge to protect sensitive data.

Service Overview

Social Engineering Testing Service evolves security testing beyond traditional methodologies to meet today's challenges. BESECURE simulates current hacker techniques used to steal sensitive data undetected through simulated phishing and date exfiltration campaigns.

BESECURE simulates e-mail spoofing fraud attempts, that is the most common method of Social Engineering, by sending realistic spear phishing emails to your employees. Each message contains a URL or crafted attachment that is unique to the recipient. Attack simulation may include email messages with attachments, URLs or messages sent via popular social networking platforms such as Facebook, LinkedIn and Twitter. The objective is to simulate the current methods hackers use to circumvent your network security and deceive your employees. The results of the assessment is used to evaluate your organization's effectiveness at defending against email and social networking attacks and determine the best method to improve your employees security awareness.

Features

– Utilize common pre-formatted phishing templates including password reset/expiration notification, social networking messages, or custom-made targeted messages.
– Detect social engineering vulnerabilities before hackers can exploit them.
– Identify physical and physiological weaknesses and vectors of attack.
– Uncover weaknesses related with employee security breaches that can lead to disclosure of sensitive data.
– Address the risk of Social Engineering rapidly evolving threat as part of an overall risk management strategy, helping organizations to strengthen employee's commitment to a security-aware culture.
– Combine on-line security awareness training offered from BESECURE e-Learning platform to educate users to avoid falling victims of spear phishing attacks.

Benefits

– Protect your organization against emerging threats.
– Reduce the risk from targeted phishing and malware attacks.
– Determine the effectiveness of your security awareness training.
– Determine how vulnerable your users' web browsers are to the exploits that attackers are using today.
– Increase your employees' knowledge to protect sensitive data.

Rich Reporting

BESECURE Social Engineering Testing reporting provides feature rich results by company, department, role, location and more
– Get details on which users were sent the phishing attack, which clicked on it, who had their credentials stolen etc.
– View campaign performance across your organization by department, region and more

About BESECURE

BESECURE, a leader in Governance Risk and Compliance solutions and services, provides Compliance Services based on legal and regulatory requirements, designs and implements advanced IT security solutions, delivers information Security Training Seminars, provides Managed Security services, performs Penetration Tests and Vulnerability Assessments covering all phases of the life cycle of information security. BESECURE applies a certified Quality Management System according to ISO 9001 and a certified Information Security Management System according to ISO 27001. For more information, please visit http://www.besecuregroup.com