Social Engineering

We conduct a simulated email spear phishing exercise over an approved sample of users. The purpose of the exercise is to send convincing spear phishing emails to assess the security awareness of your employees, managers, and executives.

1. Reconnaissance

We perform an analysis of commonly used remote access points, webmail services, employee portals, and collaboration platforms to create a sampling of scenarios designed to entice employees to do one or more of the following activities:

- Enter their Windows domain credentials into a convincing login prompt
- Download a malicious file or executable from an unknown website
- Open an emailed Microsoft Office document and accept security warnings

We then create a "Faceprint" of potential employee email addresses that we identify using open source intelligence (OSINT) toolsets, publicly available databases and targeted Internet search queries. We present this list to you for analysis and determine which email addresses you would like included in the campaign.

2. Spear Phishing Campaign

Once a scenario is agreed upon, we only target a list of approved individuals for the email-based social engineering test. If successful, we attempt to verify any credentials obtained and establish temporary access to a phishing victim's system for the purposes of demonstrating access to systems and data from the phishing attack. This exercise will not introduce actual malware or viruses to the network. Optionally, we can collaborate with you to send or display "teachable moment" messages after the exercise has completed.

3. Phone Call Social Engineering

We design phone call social engineering test cases targeting the service desk and select employees, which will typically focus on obtaining control of user accounts by asking for user names and passwords or password resets. We use persuasive techniques to encourage targets to comply with the exercise.

4. Evidence & Recommend

We present statistics from the exercise including number of emails successfully sent and received, number of links clicked, files downloaded, attachments opened, credentials obtained and successful connections established. We also provide a timeline of activities and note if/when the campaign was reported to the security team. We make recommendations for improvement to detection and response processes and user awareness messages.

Contact Us

Phone: 215.867.9051
Email: info@securityriskadvisors.com
Website: www.securityriskadvisors.com

Related Services

Technical Defenses Assessment

We assess the impact of a user falling victim to a convincing, dedicated email spear phishing attack. We simulate multiple email spear phishing methods and technical payloads on a test system, in order to assess the network, email filtering and desktop security controls intended to help protect user systems from phishing compromise. We then review your advanced threats monitoring tools and processes, including the placement and use of tiers of advanced threat controls including network and/or endpoint detection and response, payload analysis and exploit mitigation. We recommend improvements to both preventative and detective controls as appropriate, which may include process and/or toolset updates.

Executive Spear Phishing

Also known as "Whaling," we perform targeted email spear phishing exercises against a sample of your company's Executives who are most likely to have access to confidential data, passwords, financial information, etc.

About Our Company

Security Risk Advisors provides expert consulting services with specializations in advanced threats controls implementation and 24x7 operation, red and blue teams, control frameworks, and GRC process improvement. Our approach emphasizes ongoing knowledge transfer and access to our analysts.