Introduction Social Engineering Assessment

Though technical threats are often the primary concern of a security audit, many times malicious attackers threaten employees personally, trick them into providing passwords, or installing malware.

This assault – known as social engineering – will range from basic email phishing to complex operations utilizing various contact strategies.

Infopercept provides a variety of expert-driven social innovation commitments to assess both staff preparation and technological controls.

If it's conventional spear phishing (email), vishing (voice calls), or on-site inspection and trying to reach the actual building, we've qualified experts readily available.

Assessment Types

- Spear phishing (Directed Email Campaigns)
- Vishing (Incorporating Voice Calls)
- On-site Engagement (Tailgating, dropping USB drives, etc.)

Phishing in Advanced Campaigns

Often straightforward social engineering commitments are fruitful by deliberately exploiting confidential information or access, but not all attacks are so straightforward. In the case of more advanced commitments, operators can request simple office material, such as the organizational structure or who is on vacation.

This information serves as building blocks for coercing more prepared users, using common experience to gain trust and credibility.

Conducting a social engineering evaluation with Infopercept will identify the risks and effects of social engineering as well as the potential of the organization to respond to such an attack.

Assessment Details and Methodology

At Infopercept, each commitment to social engineering implements a validated approach to ensure strongly focused, reliable commitments. Each engagement shall be carried out in the following steps:

Information gathering on target organization and personnel

1.Reconnaissance

The collection of information is a crucial step of social engineering which also influences the progress of the remainder of the evaluation. Using the black box' technique, our intelligence analysts carry out in-depth analysis to collect information from the target organization.

Create pretext scenarios, preparing for execution

2.Create Pretext Scenarios and Payloads

If the objective has been thoroughly enumerated, the emphasis is on drawing up the payload. These specifics include the identification of departments, user positions, and the related pretext scenarios. These specifics mean that each customer is carefully researched for the most effective, tailored commitments.

Engage targets, safely exploiting phishing pages

3.Engage Targets

Using strategically structured strategies and pretexts, intelligence researchers at Infopercept engage workers by phishing emails or phone calls. For on-site assessments, several experiments are started, such as tailgating users and baiting staff with 'missing' USB drives in the office.

Detailed, risk- prioritized report with remediation steps

4.Assessment Reporting and Debrief

After the completion of the initiative and the aggregation of outcomes, a final report shall be submitted, containing both an executive overview and specific information.

Remediation measures and training instructions are also given to guide the customer in the resolution of the training and policy problems found.

(Optional) Social engineering training and education for employees

5.Employee Education

As an optional extension, Infopercept offers user training workshops for clients' staff. Whether hosted in a filmed online webinar or in-house training session, Infopercept offers premium security awareness training – by the same experts who did the initial work.

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/knowledge/datasheets