ZERODAYLAB®

Security Awareness Simulation:

Social Engineering

Trusted Advisor for All Your Information Security Needs

ZERODAYLAB®

Your Employees & Social Engineering: How at Risk is Your Business?

Security breaches of corporate IT networks are often thought only to come as a result of a malicious attack from technically competent computer hackers. However, social engineering often plays a large part in helping hackers bypass the initial IT security barriers.

Overly helpful employees lacking cyber security awareness often provide access to corporate offices, restricted areas and IT systems where the hacker has no authorised access.

By posing as a legitimate employee or third party, the ZeroDayLab engineer will use false credentials to trick legitimate users into divulging useful information. This information can be used to break into the corporate IT systems. Social engineering is performed by many means; by telephone, social media, phishing or by visits to corporate offices.

+44 (0)207 979 2067 | www.zerodaylab.com | info@zerodaylab.com
www.zerodaylab.nl

ZERODAYLAB®

Social Engineering Methodology

Our approach is based on an Open Social Engineering Framework testing methodology. The assessment is divided into seven steps.

1. Client Brief

The client is briefed by our senior project consultant to discuss the purpose of the assessment with the customer and to confirm the agreed Scope of Works. Rules of engagement are discussed and general admin requirements are confirmed. The consultant performing the assessment will introduce themselves via email before the social engineering test is initiated.

2.Threat Modelling

The ZeroDayLab Consultant will take the client's requirements and research these in order to formulate a threat model that will be used as the basis of the assessment.

3. Attack Scenarios

Once the threat model is formulated, ZeroDayLab then constructs the bespoke attack scenarios based upon the threat model. Various attack scenarios are considered and researched before a decision is made on which attack scenarios to use and the likelihood of success.

4. Active Engagement

At this stage the social engineering consultants carry out the attack scenarios. These may be remote and performed over the telephone or internet, or local and performed at the client's head office or remote satellite offices.

5.Client Debrief

The consultant will contact the client at the end of the assessment and the initial general feedback will be presented.

6. Report Creation

The consultant creates an in-depth report focussing on providing the business with needs-driven solutions to any issues identified. The report consists of a comprehensive PDF written report and a separate presentation highlighting the key messages identified during the assessment.

7. Report Presentation

The written PDF report and presentation are securely delivered to the client. The Consultant arranges a mutually convenient time to deliver the presentation via web conferencing to deliver the results and key messages and to answer any questions the customer may have after digesting the report.

It may be necessary for the client to request a follow-up assessment after a given time period in order for the effectiveness for any remediation to be assessed.

Why Work with ZeroDayLab?

At ZeroDayLab®, we are Passionate About Total Security Management and are committed to complete customer satisfaction.

As a CREST accredited organisation, we have grown our business year-on-year by providing our clients with a holistic approach to their IT Security posture through a comprehensive suite of consulting services and complementary security solutions.

We are proud to have leading European clients in key vertical markets such as Transport & Logistics, BFSI, Retail, and E-Commerce organisations. We are an established, well respected privately-held company with a renowned reputation for quality, confidentiality, and consistently delivering proven results for measurable ROI.

ZeroDayLab is a leading provider of comprehensive Penetration Testing, Vulnerability Assessment and Application Assessment Services as well as GRC, Education & Training and Managed Services. We have a dedicated team of security consultants that deliver a best-in-class testing capability, as well as trusted remediation, advice and guidance in the event of a breach.

- Penetration Testing:
  Internal & External Web & Mobile Applications
- Vulnerability Assessments:
  Desktop, Servers, Infrastructure
- Internal & External Security Audit
- Source Code Review
- Digital Forensic Analysis
- Architecture & Infrastructure Review
- Security Awareness Programmes
- Security Training for Developers
- Incident Response & Runbook Training
- Phishing Resilience Programmes
- Bespoke Senior Exec Security Training
- Physical Security Awareness
- SERM - Supplier Evaluation Risk Management
- ZeroDayResponse - Incident Management
- Cyber Threat Intelligence (Dark Web)
- Protective Monitoring (SOC)
- Advanced Email Security Solution
- GRC Maturity Assessments
- PCI DSS Remediation Support
- GAP Analysis to ISO & PCI DSS
- 360° Reviews
- ISO/NIST/EUGDPR Alignment
- Internal Audits
- SIEM 2 - Event & Log Management
- ISMS
- Privileged User & Identity Management
- Advanced Threat Protection, Application Whitelisting, End Point Protection.

+44 (0)207 979 2067 | www.zerodaylab.com | info@zerodaylab.com
www.zerodaylab.nl

ZERODAYLAB®

Passionate About Total Security Management

ZeroDayLab Worldwide

London
Brighton & Hove
Manchester
Dublin, Ireland
Amsterdam, The Netherlands
Bangalore, India
Wilmington, Delaware USA

London
Head Office
83 Victoria Street
London
SW1H 0HW

Brighton & Hove
Finance & Operations
96-98 Church Road Hove
East Sussex
BN3 2EB

+44 (0) 207 979 2067
info@zerodaylab.com