Security Awareness Simulation:
Social Engineering

Trusted Advisor for All Your Information Security Needs
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.

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
2. Intensive job scoping and research to create a bespoke threat model
3. Formulation of bespoke attack scenarios based on client threat modelling
4. Active social engineering engagement
5. Client debrief
6. Report creation
7. Report presentation

13% of large organisations had a security of data breach relating to social networking sites.*

* HM Government 2015 Information Security Breaches Survey
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.

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.

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.

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.

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

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.

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 Use ZeroDayLab?

As one of Europe’s leading IT Security Consulting companies, ZeroDayLab has been carrying out IT Security Testing engagements combined with complementary IT Security Solutions for a broad range of public and private sector companies with over 240+ engagements per year. Our depth and breadth of experience enables us to deliver high quality assignments that both identify all areas of your IT Security posture whilst also providing appropriate remediation and recommendations that tighten your overall security strategy on time and in budget with consistent quality and return on your investment.

At ZeroDayLab, every day is spent helping make our client’s infrastructure and applications more secure through the intelligent combination of highly trained consultants and services combined with leading edge, complementary security technologies that drives ‘Continuous Security Improvement’.

We maximise ROI by delivering value for money services and solutions of the highest and consistent quality.

ZeroDayLab has a strong set of testimonials across a broad range of industries and sectors. If you are as passionate as we are about Total Security Management, then our team of highly skilled and experienced Security Consultants will be happy to discuss your requirements in more depth and define an appropriate IT security strategy suitable for all of your business needs.

Our experienced management team consistently delivers timely and accurate IT consulting services for our clients and retain trusted advisor status in UK and across EMEA.

Our team looks forward to sharing our vision with you and helping you to defend against the malicious attacks that come from both inside and outside of your environment.

- Vulnerability Assessment of your Desktop, Servers and Infrastructure
- Penetration Testing of all your Internal & External Web Applications
- Architecture & Infrastructure Review with Recommendation and Remediation
- Source Code Review
- Forensic Analysis
- Business Continuity & Brand Protection
- Continuous IT Security Improvement Programmes
- Education & Training / Learning & Development
- Social Engineering
- IT Security Review of Policies & Procedures, Planning, Risk Assessment and Mitigation
- SIEM 2 – Event & Log Management
- ISMS / Governance, Risk & Compliance
- Incident Response & Incident Management, Proactive Threat Protection
- Privileged User Management, Traceability, Access Control
- Privileged Identity Management & Password Protection
- Advanced Threat Protection, Application White Listing, End Point Protection
- SERM – Supplier Evaluation Risk Management Solution
- ZeroDayResponse - Incident Management
- Next Generation SOC
- 360° Threat Protection
- Deep & Dark Web Intelligence
Our Partner Solutions

assuria  glasswall™  WALLIX  LIEBERMAN SOFTWARE

SIEM 2 Technology  Proactive File Remediation  Privileged User Management  Privileged Identity Management

Bit9 + CARBON BLACK  MANDIANT  MODULO  intelliagg

End Point Protection  Incident Response Management  GRC  Dark Web Intelligence

Passionate About Total Security Management

ZeroDayLab Worldwide

London
Brighton & Hove
Manchester
Eindhoven, The Netherlands
Bangalore, India

London
Head Office
83 Victoria Street
London
SW1H 0HW

London

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

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

www.zerodaylab.com