Strukturierte Social Engineering Abwehr

Wir bieten methodische Erhebungen von Bedrohungen und individuell erstellte Abwehrmaßnahmen, beides basierend auf unseren Serious Games.

Schluss mit Langeweile

Wir wollen die Menschen in Ihrer Organisation spielerisch in die Social Engineering Abwehr einbinden. Training, das Spaß macht, ist nachhaltig. Durchbrechen Sie mit uns den derzeitigen Trend von langweiligen Folienschlachten.

Forschung

Unser Angebot basiert auf wissenschaftlichen Forschungsarbeiten. Wir erforschen ständig weitere Aspekte des Social Engineering. Auf Anfrage lassen wir Ihnen gerne unsere aktuellen Forschungsergebnisse zukommen.

Support für Normen

Wir beraten Sie gerne bei der Erstellung, Konzeption und Dokumentation im Rahmen von standardisiertem Sicherheitsmanagement nach ISO 27001 oder anderen Vorgaben wie z.B. dem IT-Sicherheitsgesetz. Wir erweitern unser Angebot gerne auf weitere Standards, entsprechend Ihrem Bedarf.

6. Deutscher IT-Sicherheitspreis 2016

Auszeichnung

Die Horst Görtz Stiftung vergab am 6. Oktober 2016 zum 6. Mal den Deutschen IT-Sicherheitspreis. Eine Expertenjury aus anerkannten IT-Sicherheitsfachleuten wählte aus 45 Einreichungen die besten markt-relevanten Innovationen zur IT-Sicherheit und prämierte unsere Lösung mit dem 3. Platz.

SOCIAL ENGINEERING ACADEMY

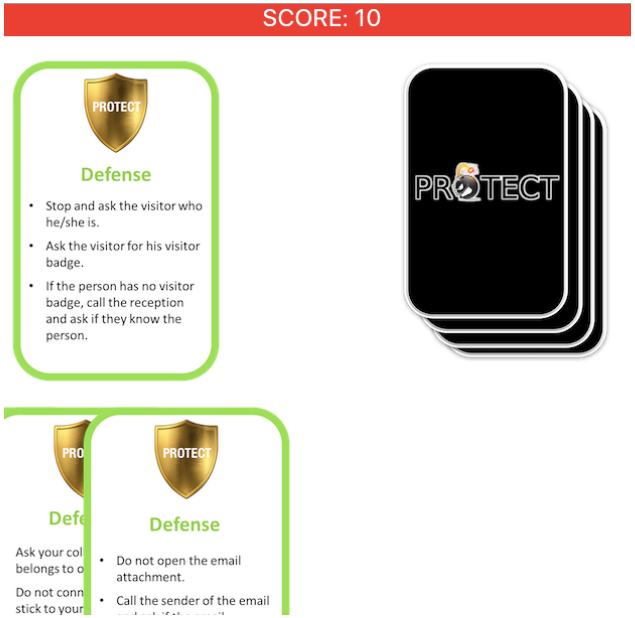
Verstehen Sie Ihre Bedrohungslage mit Hilfe unserer Serious Games

Vor einem Awareness Training erfolgt bei uns eine Bedrohungsanalyse. Das Wissen über Social Engineering Schwachstellen in Ihrem Unternehmen liegt implizit bei Ihren Mitarbeitern vor. Diese kennen die wirklichen Prozesse Ihres Unternehmens am besten. Mit unserem Serious Game HATCH bieten wir im Rahmen eines Inhouse Trainings eine strukturierte Methodik an, dieses Wissen sichtbar zu machen. HATCH versetzt die Spieler in die Rolle des Social Engineering Angreifers. Ein gut abgestimmtes Sample aus allen relevanten Abteilungen reicht hierbei aus, um die wichtigsten Bedrohungen für Ihr Unternehmen zu entdecken.

Über die Bedrohungsanalyse hinaus kann HATCH mit vordefinierten Szenarien auch für ein VIP-Training für besonders exponierte Personen (z.B. Buchhaltung / Projektleitung) verwendet werden.

Richten Sie Ihr Security Awareness Training an der Bedrohungslage aus

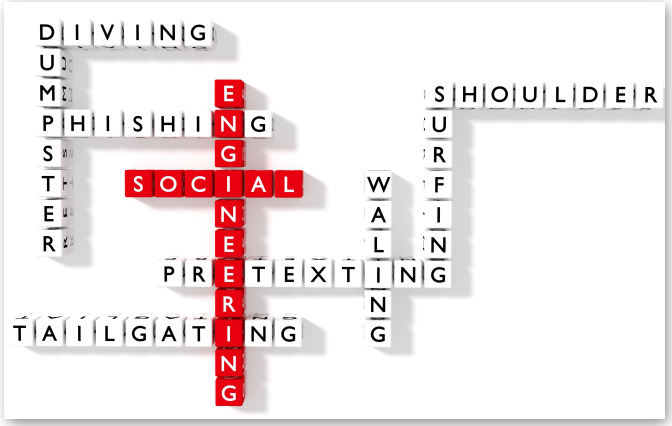
Aus den individuellen Bedrohungen für Ihr Unternehmen erstellen wir eine ebenfalls auf Ihr Unternehmen zugeschnittene Version unseres Serious Games PROTECT. Das Online Game wird allen Mitarbeitern Ihrer Unternehmung zur Verfügung gestellt. So erreichen Sie eine kostengünstige Skalierung Ihres individuellen Security Awareness Trainings. In dem Spiel müssen die Spieler Bedrohungen abwehren.



Unsere Platform generiert Zertifikate für die erfolgreiche Teilnahme. Ein HighScore erlaubt einen spielerischen Wettbewerb zwischen den Teilnehmern. Unsere Datenschutzerklärung erläutert die Verwendung aller Daten im Detail.

Verbessern Sie die Qualität Ihrer Abwehrmaßnahmen kontinuierlich

Unsere Methodik ist effektiv gegen alle Arten des Social Engineering wie Phishing oder CEO Fraud. Sowohl die Bedrohungsanalyse, als auch das Awareness Training umfassen alle Varianten des Social Engineering und werden permanent von uns aktualisiert.



Wir bieten als weitere Leistung an, Ihre Bedrohungslage mit Ihrer IT-Security Policy abzustimmen. Mit der Unterstützung unserer Partner haben wir auch weiterführende Dienstleistungen, wie automatisierte Phishing Tests, im Angebot.

Kontakt:
Social Engineering Academy (SEA) GmbH
Eschersheimer Landstraße 42
60322 Frankfurt am Main
Tel.: 069-945195240
Web: https://www.social-engineering.academy
Email: info@social-engineering.academy