HATCH

Ein Serious Game zur Social Engineering Abwehr

Awareness Training

Unser Awareness-Training bietet neben dem Einsatz des Spiels kurze Vorträge zu Angriffen sowie deren Diskussion in der Gruppe. Zudem können an passender Stelle aktuelle Sicherheitsrichtlinien mit den Mitarbeitern diskutiert werden, um sie auf ihre Sinnhaftigkeit zu prüfen. Dies führt häufig zu einer Verbesserung und Akzeptanz der Richtlinien.

Bedrohungsanalyse

Eine umfassende Bedrohungsanalyse für Social Engineering wird durch den Einsatz unseres Spiels möglich. Wir können somit Angriffe auf Endkunden, Mitarbeiter, IT Experten usw. untersuchen und die Ergebnisse zur Gesamteinschätzung der Bedrohungssituation aggregieren.

Standard Compliance

Wir bieten Beratungen bei der Dokumentationserstellung im Rahmen vom standardisiertem Sicherheitsmanagement nach ISO 27001 oder anderen Vorgaben wie z.B. dem IT-Sicherheitsgesetz. Wir erweitern unser Angebot gern auf weitere Standards, je nach Bedarf unserer Kunden.

Interaktives Training

Kernstück unseres Trainings ist das Kartenspiel HATCH (Hack and Trick Capricious Humans), das jedermann in die Lage versetzen soll, Trickbetrüger (die sich beispielsweise als Telekom-Mitarbeiter ausgeben und zur Installation von Software auffordern) zu erkennen und den Angriff abzuwehren. Durch einfache Anwendbarkeit kann den Spielern so die grundlegende Funktionsweise von Betrugsmaschen im Training verständlich gemacht werden.

Unser Training bietet eine unterhaltsame Security Awareness Maßnahme, die spielerisch Menschen die Gefahren durch Social Engineering verdeutlicht und sie kontextbezogene Bedrohungen analysieren lässt. Die Nutzung von Serious Gaming für die Abwehr von Social Engineering fundiert auf der Basis von wissenschaftlicher Literatur und ist eine

SOCIAL ENGINEERING ACADEMY

3. Platz belegt beim Deutschen IT-Sicherheitspreis

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

Szenarien

Wir bieten reale und fiktive Szenarien an. Reale Szenarien erlauben das Auffinden von spezifischen Bedrohungen für Mitarbeiter und für die Unternehmung. Fiktive domänenspezifische Szenarien erlauben keine Analyse von Bedrohungen auf spezifische Mitarbeiter, aber erleichtern das Übertragen des Gelernten auf den Alltag. Im Gegensatz zu Social Engineering Penetration-Tests werden bei uns Mitarbeiter nicht bloßgestellt. Unsere Spielwelt wird stets individuell auf Kundenwünsche anpasst.

Sprachen

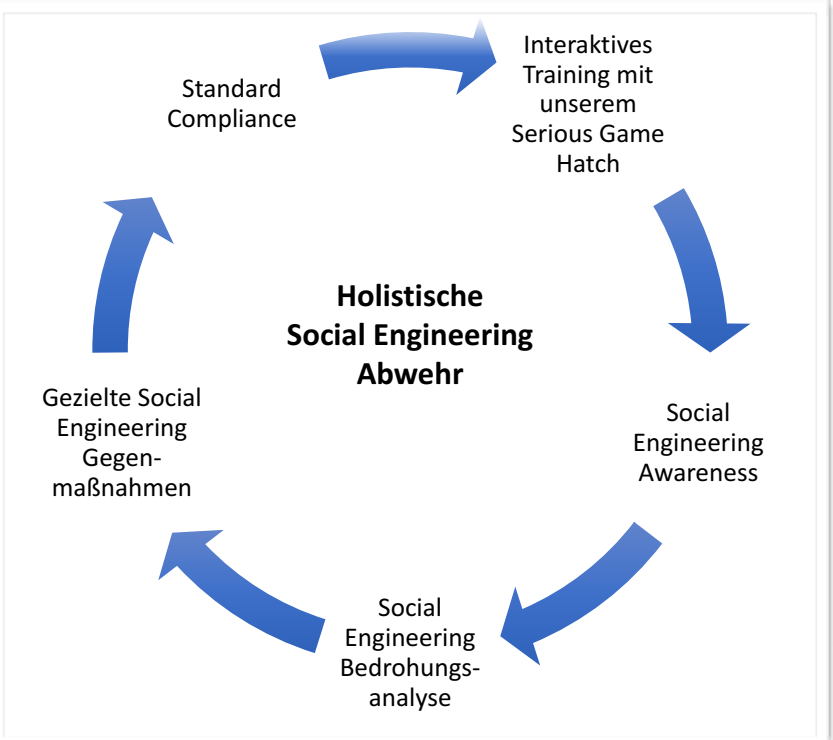
Deutsch, Englisch, Mandarin

Neuheit auf dem Gebiet der Security Awareness. Wir bringen somit Spielspaß, theoretische Fundierung und Abwehr gegen Social Engineering in einer simplen Lösung zusammen.

Durch die Umsetzung der Trainingsmaßnahme als Kartenspiel werden die Spieler bewusst in eine andere Umgebung gebracht und können dort (mit etwas Abstand zum Tagesgeschäft) die prinzipielle Funktionsweise von Social Engineering Angriffen ausprobieren und somit verstehen.

Holistische Social Engineering Abwehr

Wir bieten ein aufbauendes Program von Maßnahmen an, das mit dem Training mit dem Serious Game HATCH beginnt. Unsere Trainings steigern zunächst die Awareness der Mitarbeiter und die Motivation, sich mit dem Thema zu befassen. Eine weitere Auswertung der beim Spielen gesammelten Daten erlaubt eine genaue Bedrohungsanalyse. Da die Mitarbeiter sich dabei mit Social Engineering auseinandersetzen, ist es nicht notwendig einem Social-Engineering-Experten alle Arbeitsprozesse zu erläutern. Gleichzeitig erhöht unsere Methode die Awareness der Mitarbeiter und erlaubt eine fortlaufende Schulung und Analyse. Auf Basis der Bedrohungsanalyse erfolgt eine Verbesserung der Abwehr durch zielgerichtete Gegenmaßnahmen. Diese Maßnahmen schützen das Vermögen und die Daten von ihrer Firma.



Abschließend kann die Dokumentation in die Umsetzung von Security Standards einfließen. Die Umsetzung von Sicherheitsstandards wie z.B. ISO 27001 ist eine nicht triviale Aufgabe. Insbesondere bietet diese Norm, wie viele andere ebenfalls, keine Hilfestellung bei der Feststellung von Bedrohungen durch Social Engineering oder der Umsetzung von Gegenmaßnahmen wie etwa dem ISO 27001 Control A.7.2.2 - Information security awareness, education and training. Auch im Rahmen des IT Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik kann unser Spiel als Gegenmaßnahme zur Bedrohung G 5.42 Social Engineering dienen.

Evaluation

Die Evaluation unseres Spiels erfolgte in mehreren Schritten. Zunächst haben wir die kontextbezogene Version mit einem realen Szenario mit 25 Vollzeitangestellten mit einem Hochschulabschluß der Technischen Universität München und der Goethe Universität in Frankfurt gespielt. Die Spieler haben insgesamt 49 Runden gespielt in denen Bedrohungen vorgeschlagen wurden. Von diesen wurden 42 als möglich und 7 als nicht möglich eingestuft. Diese Zahlen zeigen, dass es den Spielern erfolgreich gelang Bedrohungen zu ermitteln (weitere Details in [1]).

Im Anschluss haben wir einen Versuch mit 105 Studenten der Technischen Universität München durchgeführt. Die Studenten spielten eine Version des Spiels mit dem Büro Szenario. Die Teilnehmer haben vor und nach dem Spiel Fragebögen ausgefüllt, die Wissen über Social Engineering sowie Wissen, Einstellung und geplantes Verhalten im Bezug auf Security Awareness erfassen (vergleiche [2]). Die Teilnehmer wurden gebeten auf einer 5-stufigen Likertskala von “vollständige Ablehnung” bis “vollständige Zustimmung” zu antworten. Das Spielen unseres Spiels hat insgesamt zu einer signifikant erhöhten Security Awareness geführt ($M = 3.73$, $SD = .62$) im Vergleich zu den Messungen vor dem Spiel ($M = 2.73$, $SD = .31$), mit $t(9)=-4.52, p = <.001$.

Ebenfalls haben die Teilnehmer angegeben, nach dem Spielen mehr Wissen über Social Engineering zu haben, beim Spielen neue Inhalte gelernt zu haben und sogar, dass die Spieler dieses Wissen in ihrem Alltag anwenden können. Eine Evaluation mit über 100 Teilnehmern aus der Industrie mit einem vergleichbaren Ergebnis wird in Kürze erscheinen.

[1] K. Beckers and S. Pape, “A serious game for eliciting social engineering security requirements,” in Proceedings of the 24th IEEE International Conference on Requirements Engineering, RE ’16, IEEE Computer Society, pp. 16-25, 2016.

[2] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” Comput. Secur., vol. 25, no. 4, pp. 289–296, 2006.

Kontakt

Dr. Kristian Beckers (München)
- Email: kristian.beckers@social-engineering.academy
- Telefon: + 49 69 9451952 40

Dr. Sebastian Page (Frankfurt)
- Email: sebastian.pape@social-engineering.academy
- Telefon: + 49 69 9451952 40