Juristische Bewertung eines Social-Engineering-Abwehr-Trainings

D.-K. Kipker, S. Pape, S. Wojak, K. Beckers

Forschungsprojekte:
SIDATE & VeSiKi

Social Engineering

Bei Social Engineering (SE) wird durch Beeinflussungen der Opfer versucht, ein bestimmtes Verhalten hervorzurufen und auszunutzen, um sensible Informationen zu beschaffen. Laut dem aktuellen Datensatz des Data Breach Investigations Report [1] enthalten 43 % aller Datendiebstähle einen SE-Angriff. Dabei ist der SE-Angriff oft der erste Schritt eines größeren Angriffs, bei dem der Angreifer die dort gewonnen Informationen für weitere Angriffe verwendet.

Trainingsmaßnahmen zur Social-Engineering-Abwehr

Zurzeit haben Firmen hauptsächlich zwei Strategien, um SE-Angriffe abzuwehren: Einerseits können sie Penetration-Tester beauftragen, die als „gutartige Hacker" die Mitarbeiter angreifen und dabei Schwachstellen finden sollen. Leider ist dieser Ansatz nicht ganz unproblematisch. Experimente haben gezeigt, dass dieser Ansatz auch dazu führen kann, dass Angestellte demotiviert werden, wenn sie mit den Ergebnissen des Tests konfrontiert werden. Außerdem kann ein derartiger Test in das Persönlichkeitsrecht der Mitarbeiter eingreifen, sodass es zahlreiche arbeitsrechtliche Anforderungen an SE Penetration-Tests gibt [2, 3]. Andererseits können Firmen Schulungen und Security-Awareness-Trainings durchführen, in denen die Mitarbeiter auf Socia-Engineering-Bedrohungen hingewiesen werden. Oft sind diese Schulungen verpflichtend, haben aber keinen lang anhaltenden Effekt [4].

Eine dritte Möglichkeit sind Serious Games, d. h. Spiele, die neben Unterhaltung auch ein ernsthaftes Ziel verfolgen. Diese können zum Beispiel für Awareness-Trainings eingesetzt werden, um Mitarbeiter auf mögliche IT-Sicherheitsbedrohungen aufmerksam zu machen.

HATCH

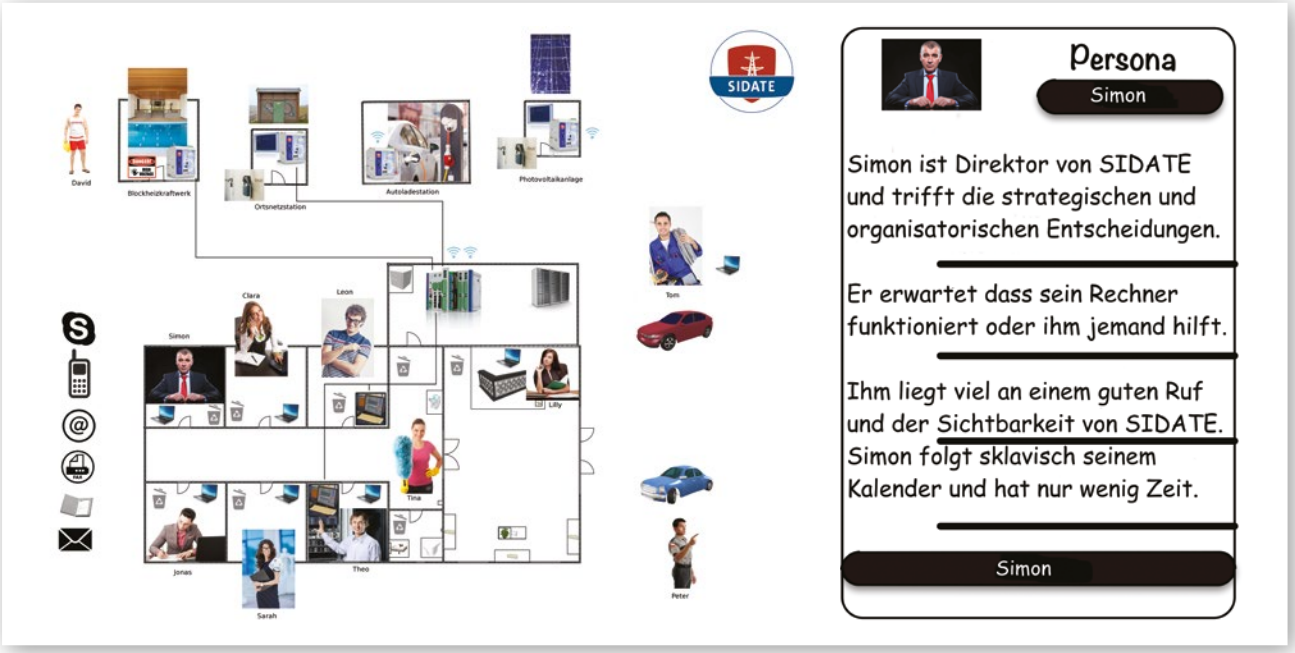
Eines der beschriebenen Serious Games ist HATCH (siehe Abbildung 1), das das Verständnis der Arbeitnehmer von SE verbessert [5]. Durch das Spiel kann außerdem eine Liste möglicher SE-Bedrohungen erstellt werden, die zur Verbesserung der Sicherheit dienen kann [6]. Je nach Ziel wird mit einem ausgedachten (virtuellen) Szenario oder einem (realistischen) Szenario, das das reale Arbeitsumfeld abbildet, gespielt.

Virtuelle Szenarien

Beim Einsatz von HATCH zu Schulungs- und Awarenesszwecken kommen virtuelle Szenarien zum Einsatz. Diese bestehen aus einem Plan einer Abteilung oder Firma (siehe Abbildung 2 links) und für jede der im Plan dargestellten Mitarbeiter existiert eine Persona-Karte, die die grundlegenden Eigenschaften des Mitarbeiters skizziert (siehe Abbildung 2 rechts). Aufgabe der Spieler ist es nun, sich einen auf Basis der gezogenen Karten möglichst plausiblen Angriff auszudenken, der die Eigenheiten der im Spiel vorhandenen Mitarbeiter ausnutzt. Der gefundene Angriff wird dann von den Mitspielern auf Plausibilität bewertet.

Abb. 1: HATCH im Einsatz auf dem ITS-KRITIS Workshop

Abb. 2: Ein Spielplan von HATCH (links) und eine Persona-Karte (rechts)



Realistische Szenarien

Der grundlegende Spielablauf von HATCH mit einem realistischen Szenario ist derselbe wie mit einem virtuellen Szenario. Allerdings kommen hier keine virtuellen Personen zum Einsatz, stattdessen wird ein Plan der realen Arbeitsumgebung erstellt und die Spieler denken sich Angriffe auf ihre Kollegen aus. Dabei verwenden sie das bereits vorhandene Wissen über Arbeitsabläufe, Kompetenzen und Vorlieben der Kollegen. Als Ergebnis entsteht deswegen eine Liste mit möglichen SE-Bedrohungen, die dann dazu dienen kann, Arbeitsabläufe und Sicherheitsrichtlinien zu verbessern. Der Vorteil gegenüber einer Bedrohungsanalyse von Experten besteht darin, dass die Mitarbeiter einer Abteilung oder eines Unternehmens die realen Arbeitsabläufe bestens kennen, so dass es leichter ist, sie in SE zu schulen, als Experten alle Arbeitsabläufe studieren zu lassen.

Juristische Bewertung von HATCH

Allgemein ist anerkannt, dass die Geschäftsleitung eine rechtliche Verpflichtung besitzt, Maßnahmen der IT-Sicherheit als Bestandteil der unternehmenseigenen Compliance zu unterhalten und zu betreiben – hierzu gehört auch die Schulung von Mitarbeitern im Hinblick auf Social Engineering-Angriffe. Abgeleitet werden kann die IT-sicherheitsrechtliche Compliance-Verpflichtung dabei aus den unterschiedlichsten Rechtsvorschriften und in Abhängigkeit von der jeweiligen Branche, ganz allgemein aus § 43 Abs. 1 GmbHG und § 93 Abs. 1 AktG. Wo auf der einen Seite unternehmerische Verpflichtungen zur Realisierung eines angemessenen IT-Sicherheitsniveaus bestehen, stellt sich auf der anderen Seite die Frage, ob und wie der Arbeitnehmer damit verbundene Maßnahmen dulden und gegebenenfalls auch an diesen mitwirken muss. Der Konflikt zwischen Freiheit und Sicherheit aktualisiert sich hier in der Form arbeitsrechtlicher und auch datenschutzrechtlicher Fragestellungen sowie für die unternehmerische Compliance und Corporate Governance. Speziell für ein SE-Spiel wie HATCH, das eine aktive Teilnahme des einzelnen Mitarbeiters voraussetzt, eröffnen sich deshalb verschiedene juristische Problemfelder. Zu unterscheiden ist dabei zwischen dem realistischen und dem virtuellen Spielszenario.

Realistische Szenarien

Im realistischen Szenario von HATCH spielen sich die im Unternehmen beteiligten Akteure selbst. Eine besondere rechtliche Relevanz ergibt sich für diesen Fall daraus, dass die simulierten SE-Angriffe auf reale Personen und deren Charaktereigenschaften abzielen. Für die Frage der rechtlichen Zumutbarkeit für den einzelnen Arbeitnehmer ist dabei dessen aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG folgendes Allgemeines Persönlichkeitsrecht (APR) zu berücksichtigen. Einfluss auf das Arbeitsrecht findet das APR unter anderem als arbeitsvertragliche Nebenpflicht des Arbeitgebers gem. § 241 Abs. 2 BGB. Für den Arbeitgeber streiten demgegenüber, ebenfalls auf der mittelbaren Drittwirkung der Grundrechte im Privatrechtsverhältnis beruhend, die aus Art. 12 GG folgende Berufsfreiheit und der damit verbundene Schutz von unternehmerischen Interessen. Grundsätzlich gilt, dass der Arbeitgeber im Rahmen seiner mittelbar aus dem APR folgenden Verpflichtungen den Arbeitnehmer vor rechtswidrigen Eingriffen in seine Persönlichkeitsrechte zu schützen hat [7]. Hierzu gehört auch der Schutz vor potenziell bloßstellenden Maßnahmen, die sich negativ auf die Beschäftigten auswirken können [8]. Speziell für ein SE-Spiel in einem realistischen Szenario bestehen hier Risiken, indem sich Mitarbeiter bloßgestellt oder in ihrer betrieblichen Wertschätzung herabgesetzt fühlen, indem durch ein Erleben des Spiels als realistische Situation persönliche Grenzen überschritten werden und gruppendynamisch nicht vorhersehbare Spielverläufe eintreten. Fraglich ist, ob demgegenüber und im konkreten Fall die betrieblichen Interessen an der Durchführung des Spiels überwiegen und damit die Befolgung der IT-sicherheitsrechtlichen Compliancepflicht als gegenüber dem Arbeitnehmerschutz höherrangig einzustufen ist. Hierbei gilt der Grundsatz, dass in besonders sicherheitsrelevanten Sektoren und Branchen Lücken in der Unternehmenssicherheit durchaus ein hohes Gewicht im Rahmen der Interessenabwägung besitzen [9]. Daraus lässt sich, in Abwägung der Arbeitgeber- gegen die Arbeitnehmerinteressen, für den Regelfall folgern, dass sich die mit HATCH verbundene, unter wahrscheinlichen Umständen erfolgende fiktive Schaffung eines potenziell arbeitnehmerschädigenden Umfelds, in welchem die reale Persönlichkeit des Arbeitnehmers mit für Social-Engineering relevanten Schwachpunkten exponiert wird, in nicht in besonderem Maße exponierten Betrieben nur schwerlich mit dem potenziell erhöhten Lernerfolg einer Sensibilisierungsmaßnahme zur Förderung der IT-Sicherheit wird rechtfertigen lassen. Anders wäre dies bei Kritischen Infrastrukturen mit einem hohen Angriffsrisiko bzw. bei Unternehmen, die bereits häufig Opfer von Social Engineering-Vorfällen gewesen sind und für die sich eine ähnliche Gefährdungslage auch für die Zukunft abzeichnet: Hier könnte der erhöhte Bedarf an Sensibilisierungsmaßnahmen als Sachzusammenhang mit dem Schutz der Arbeitnehmer und von deren Arbeitsplätzen eine Durchführbarkeit der Maßnahme vor allem auch im Interesse des Mitarbeiters begründen. Eine unter Umständen anders gelagerte rechtliche Würdigung kann sich auch für die Fälle einer Bedrohungsanalyse ergeben, indem die hier durchzuführende Methodik zwingend voraussetzt, dass sämtliche für die IT-Sicherheit relevanten Schwachstellen in einem Unternehmen ermittelt werden, worin deshalb zwangsläufig auch der Faktor Mensch einzubeziehen ist.

> Die IT-sicherheitsrechtliche Compliancepflicht des Arbeitgebers steht in Konflikt mit dem Schutz des APR der Arbeitnehmer

Virtuelle Szenarien

Im virtuellen Szenario von HATCH werden die SE-Angriffe anhand fiktiver Charaktere und der damit verbundenen erdachten Rollenzuweisungen gespielt. Auch hier hat, wie schon für das realistische Szenario, eine rechtliche Abwägung zwischen den Persönlichkeitsinteressen des Arbeitnehmers und den betrieblichen und wirtschaftlichen Interessen des Arbeitgebers zu erfolgen. Ein Stigmatisierungsrisiko für den einzelnen Mitarbeiter besteht hier insoweit, als durch technische oder inhaltliche Wissenslücken in Bezug auf Social-Engineering-Bedrohungen persönliche Defizite gegenüber dem Arbeitgeber offenbart werden. Dem kann jedoch durch vor dem Spiel durchgeführte Schulungsmaßnahmen zur SE-Prävention entgegengewirkt werden. Klar formulierte Kommunikations- und Spielregeln tragen ferner dazu bei, dass Situationen potenzieller Anfeindung, Schikane

oder Diskriminierung während des Spielverlaufes schon im Vorfeld effektiv begegnet werden kann. Nicht zuletzt ist aufgrund der Wahl von fiktiven Charakteren auch das Maß einer Persönlichkeitsbeeinträchtigung deutlich geringer, indem innere Strukturen und Eigenschaften des Arbeitnehmers grundsätzlich nicht Spielgegenstand sind [10]. Ebenso bietet HATCH im fiktiven Szenario eine Möglichkeit, die Persönlichkeitsentwicklung der Arbeitnehmer im Rahmen der Pflichtausübung von § 75 Abs. 2 BetrVG zu fördern und zu unterstützen. Wie im realistischen Szenario auch ermöglicht das Spiel dem Arbeitgeber, durch eine verbesserte Awareness seiner Mitarbeiter den Betrieb vor Angriffen durch Social Engineering zu schützen. Im Ergebnis überwiegen deshalb im virtuellen Spielbetrieb die Arbeitgeberinteressen grundsätzlich diejenigen des Arbeitnehmers, sodass der Einsatz von HATCH eine denkbare Alternative zu den klassischen Schulungsmaßnahmen in diesem Bereich darstellt.

Quellen

[1] Verizon (2017, Mai). Data Breach Investigations Report, 10th Edition. Abgerufen am 24. Mai, 2017, 2017. http://www.verizonenterprise.com/verizon- insights-lab/dbir/2017/.

[2] Kuhn, Jörn; Willemsen, Alexander: Arbeitsrechtliche Aspekte von Social Engineering Audits. In: DER BETRIEB, Heft 02 vom 15.01.2016, S. 111-117. https://www.wiso-net.de/document/MCDB__DBDBDB1167400.

[3] Zimmer, Mark; Helle, Alicia: Tests mit Tücke – Arbeitsrechtliche Anforderungen an Social Engineering Tests. In: Betriebs-Berater, 21/2016 vom 23.05.2016, S. 1269.

[4] Stahl, Stan: Beyond information security awareness training: It's time to change the culture. In: Information Security Management Handbook, Sixth Edition, edited by Hal Tipton and Micki Krause, Auerbach, 2006. https://citadel-information.com/wp-content/uploads/2010/12/Beyond-Awareness-Training-Its-Time-to-Change-the-Culture-Stahl-0504.pdf.

[5] Beckers, Kristian; Pape, Sebastian; Fries, Veronika: HATCH: Hack And Trick Capricious Humans – A Serious Game on Social Engineering. In Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, Juli 2016.

[6] Beckers, Kristian; Pape, Sebastian: A Serious Game for Eliciting Social Engineering Security Requirements. In Proceedings of the 24th IEEE International Conference on Requirements Engineering, IEEE Computer Society, RE ,16, September 2016.

[7] GK-BetrVG/Kreutz, Bd. 2, 10. Aufl. 2014, § 75 BetrVG, S. 99, Rn. 106.

[8] Kuhn/Willemsen, DB 2016, S. 112.

[9] Ricken, RdA 2001, S. 52.

[10] Vgl. Kittner et al., Arbeitsrecht 2015, S. 1206, Rn. 61.