Was zum Anfassen

Awareness-Circle-Training „SECURITY PARCOURS"

Wie gestaltet man Security-Trainings, die bleibende Awareness schaffen und gleichzeitig auch noch Spaß bereiten? Das Unternehmen T-Systems hat das Awareness-Training „SECURITY PARCOURS" entwickelt, in dem die Mitarbeiter in Kleingruppen mehrere Stationen durchlaufen. Der Beitrag stellt das Konzept vor.

Von Dietmar Pokoyski, Köln

Der „SECURITY PARCOURS" ist wie so viele Parcours mit Springreiten, einem Golfplatz oder einer Geisterbahn vergleichbar: Je nach Umfang gibt es vier bis sechs Stationen, das heißt Stände oder einfach nur Tische, die nach einer bestimmten Dramaturgie an einem oder an zwei Veranstaltungstagen synchron Teams mit circa 5 bis 10 Mitarbeitern empfangen. Die jeweiligen Stations-Moderatoren trainieren diese Kleingruppen in zehnminütigen Mitmach-Settings für ein Sicherheitsthema. Aktuell stehen zur Auswahl „Informations-Klassifizierung", „Clear Desk", „Besucher & Ausweise", „Password Hacking", „Informationsschutz (allgemein)" sowie „Social Engineering" und „Social Media". Zum Training, das die Teilnehmer im Stehen absolvieren, gehört, neben einer Einführung durch den Moderator, jeweils eine Aufgabe, die im Team gelöst werden muss sowie anschließend das gemeinsame Besprechen der Teamlösung. Ist die Lösung der Aufgabe richtig, gibt es Punkte zu gewinnen. Die beste Mannschaft erhält am Ende eine Auszeichnung. „Erfunden" wurden die Basiselemente dieses Konzepts bei der T-Systems Tochtergesellschaft „IT Services Hungary" und weiterentwickelt vom Security-Awareness-Team der T-Systems. Erste Tests und Veranstaltungen mit circa 500 Teilnehmern führte man in Ungarn und der Slowakei durch, später weitete man das Programm auf andere europäische Standorte aus.

Ablauf eines Parcours

Der Ablauf einer einzelnen „SECURITY PARCOURS"-Station ist stets identisch und lässt sich in drei Phasen strukturieren. In der Startphase macht der Moderator die Teilnehmer mit dem jeweiligen Thema vertraut. Dabei orientiert er sich an den vier bis sechs Regeln des Moderationsinstruments „mySecurity & Privacy Box" (vgl. Kasten). Mithilfe dieser kurz formulierten Regeln, die eine Essenz der Security-Policies bei T-Systems darstellen, lassen sich bei konsequenter Umsetzung durch die Mitarbeiter circa 80 Prozent aller Sicherheitsrisiken adressieren. Im Mittelteil, der Spielphase, kommt eine Simulation, das heißt ein etwa zwei bis vier Minuten langes Mini-Planspiel zum Einsatz, welches das komplette Team bestreitet. Ist der Durchlauf erfolgreich, gibt es Punkte.

So sollen die Teams etwa an der Station „Clear Desk" 25 Objekte beziehungsweise Dokumente von der einfachen Kaffeetasse über eine Brieftasche, mehreren Schlüsseln bis hin zu Passwortnotizen oder Bewerbungen auf eine grüne oder rote Decke sortieren, die das Liegenlassen beziehungsweise Einschließen beim Verlassen des Arbeitsplatzes repräsentieren. Eine andere Station ist das „Passwort Hacking": Wie bei einer Versteigerung sollen die Teilnehmer lautstark Begriffskombinationen rufen, die sie aus Hobbys, Lieblingsfußballklub, Haustiernamen und anderen Einträgen einer fiktiven Person aus deren Facebook-Profil entnehmen, um daraus ein Passwort zu generieren. Das „Password Hacking" gehört in der Praxis zu den lebendigsten und beliebtesten Stationen des Parcours.

Ein weiteres Beispiel: Mithilfe von diversen Zitaten auf großen Spielkarten sollen die Teilnehmer an den Stationen „Social Engineering" und „Social Media" durch bloßes Sortieren der Karten lernen, welche sozialen Einfalltore und damit Methoden sich Betrüger bedienen beziehungsweise welche Statusmeldungen in den sozialen Netzwerken arbeits- oder zivilrechtliche Konsequenzen nach sich ziehen könnten. Und an der Station „Besucher & Ausweise" geht es zwar vordergründig „nur" um das Puzzeln eines überdimensionalen Gast-Ausweises der Deutschen Telekom. Da aber aus der Wirkungsforschung bekannt ist, dass allein ein manuelles Agieren die Kommunikationsqualität verbessern kann, sind die Teilnehmer hier während ihres kreativen Wirkens um das Riesenpuzzle besonders aufnahmefähig für Belange im Kontext des Zutrittschutzes. Am Ende jeder Station reflektieren Moderator und Team schließlich die Ergebnisse der Spiele gemeinsam und es wird seitens des Moderators auf vertiefende Medien und Kanäle verwiesen.

Die Organisation eines „SECURITY PARCOURS" führt T-Systems dezentral durch, das heißt, jede

Tochtergesellschaft im Ausland muss diesen selbstständig mit eigenen Moderatoren und eigenen – gegenüber den meisten anderen Awareness-Maßnahmen allerdings relativ kostengünstigen – Marketingmitteln durchführen. Das zentrale Security-Management des Unternehmens liefert mögliche Inhalte in den bisher durchgeführten Sprachen, begleitet die Organisation über Beratung sowie Briefings und leistet für das lokale Security-Management vor Ort Support. Sämtliche Materialien für alle Stationen mit Ausnahme der optionalen Bonus-Station „Bluff&Hack“ passen inklusive des zugehörigen Begleitmaterials (z. B. Poster) in einen herkömmlichen Hartschalenkoffer mit 120-Liter-Volumen.

Sensibilisierung auf der Beziehungsebene

Das Feedback der Teilnehmer war bisher für alle durchgeführten Veranstaltungen sehr positiv. Was aber unterscheidet den Parcours methodisch von klassischen Trainings oder dem eLearning? Im Gegensatz zur digitalen Online-Sensibilisierung, zum Beispiel mithilfe eines Web-Based-Trainings (WBT), das bei aller Selbstbestimmtheit der Zielgruppe einsam stattfindet und einsam endet, hebt die Sensibilisierung durch „SECURITY PARCOURS“-Awareness von der kognitiven Ebene der reinen Informationsvermittlung auf die für das Lernen so wichtige Beziehungsebene. Der Einzelne profitiert dabei von der emotionalen Aufladung innerhalb der Gruppe. Denn soziale Teilhabe führt implizit zu einem höheren Involvement, mehr Lebendigkeit und schließlich zu einer ganzheitlichen Awareness, bei der einzelne Lernschritte über das Agieren und Interagieren mit Erlebnissen belegt werden und auf diesem Weg eine bessere Resilienz (Widerstandskraft) und Memorierbarkeit – auch in Bezug auf notwendige Automatismen – erzielt werden. Form und Inhalt des „SECURITY PARCOURS“ bilden Gesprächsthemen und bringen Sicherheit in einen kommunikativen Umsatz, das heißt, im Idealfall werden das Event und seine Detailthemen auch nach Teilnahme nicht nur innerhalb der Gruppe bewegt und weiterdiskutiert, sondern auch etliche Multiplikationseffekte unter Kolleginnen und Kollegen geschaffen, die nicht teilnehmen konnten oder wollten. Am Standort München betonten die Teilnehmer beispielsweise explizit, dass es „etwas zum Anfassen gab und deshalb besonders hängen bleibt“.

Awareness-Stufen

Das methodische Framework des Trainings ist jedoch kein Zufall, sondern beruht auf Erfahrung und qualitativen wie quantitativen Awareness-Evaluationen bei T-Systems. Dass Mitarbeiter in Kopf und Seele keinen „Kassettenrekorder“ eingebaut haben, den man lediglich mit Schulfernsehen-Kassetten füttern muss, fand das Security-Management bei der Planung der ersten Security-Kampagne 2006 heraus. Daher übersprang man einfach Stufe eins der Mitarbeiter-Awareness, die klassische Lerntheorie, zugunsten der Stufe zwei. Diese Stufe zwei zeichnet sich aus durch marketing-orientierte Maßnahmen mit aufmerksamkeitsstarken Promotion-Tools, die im Sinne einer integrierten Kommunikation produktiv und widerspruchsfrei miteinander harmonieren. Das Projekt nannte man „Mission Security“; Leitfigur war der sicherheitsaffine „Projektleiter“ James Bit, der während der Kampagne die Mitarbeiter des Unternehmens durch ein breites Portfolio an Maßnahmen führte, das die im ersten Jahrzehnt des neuen Millenniums stark veränderten Medienverfassungen ##Mediennutzung?## der unterschiedlichen Zielgruppen bediente.

2010 reagierte man bei T-Systems abermals auf kulturelle Entwicklungen: Empirische Untersuchungen belegten, dass die Sensibilisierungserfolge - vor allem via digitaler Medien - eine emotionale Aufladung benötigen, um nicht zu verpuffen. Daher kreierte man die „mySecurity & Privacy Box“ mit 70 elektronischen Moderationskarten (eCards) zu insgesamt sechs Themenfeldern. Ziel war die Integration von auditierbaren Moderationsrunden in die Team-Meetings über die Führungskräfte als Moderatoren, sodass bereits im Kontext der Box ein stärkerer Dialog mit den Menschen im Fokus der Bemühungen stand.

Der „Königsweg“ auf die dritte Stufe (Awareness 3.0) der Mitarbeiter-Sensibilisierung zeich-

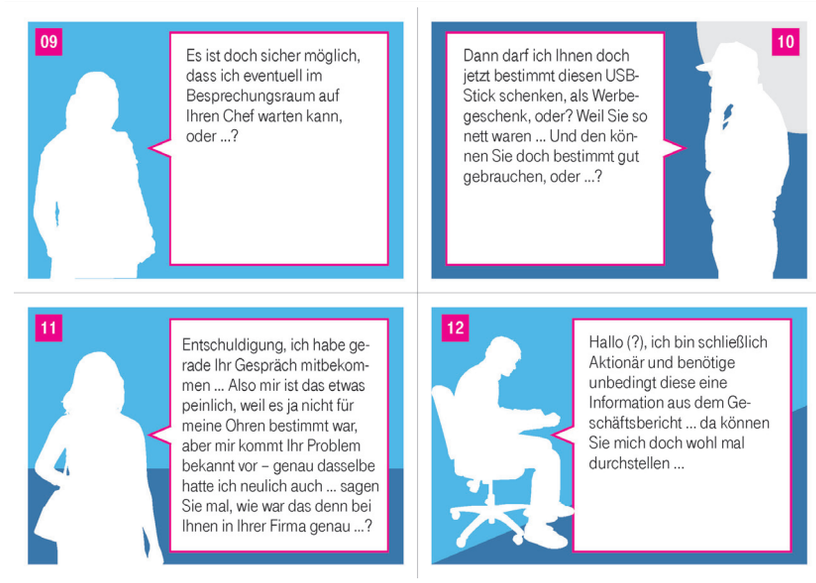

Abbildung 1: An der Station „Social Engineering“ sollen die Teilnehmer Karten mit Zitaten sortieren und so die typischen Methoden kennenlernen.

net sich nun aus durch die planvolle Integration systemischer Kommunikation, also die Kommunikation mit sich selbst und mit anderen unter Einbeziehung von Erkenntnissen aus der Gestalt- beziehungsweise Tiefenpsychologie. Da Awareness gerade dort nicht nur Sensibilisierung, sondern auch das Bewusstsein für das eigene, selbstbestimmte Handeln meint, geht es auf dieser Stufe um das Ziel, die Selbstwahrnehmung – hier natürlich im Kontext von Sicherheitsfragen – ebenso zu verbessern wie den kommunikativen Umgang innerhalb des eigenen Teams zum Wohle einer produktiven und widerstandsfähigen Information Security.

Durch den strategisch bewusst gewählten Einsatz der sozialen Teilhabe im Rahmen von Mitarbeiter-Sensibilisierung über das aktuell laufende Maßnahmenpaket „Mission Security III“ setzt T-Systems also weiterhin auf Awareness 3.0. Für 2013 sind weitere „SECURITY PARCOURS“ geplant, zum Beispiel in Deutschland, UK, Russland und Asien. Darüber hinaus fordert der Mitarbeiter-Wettbewerb „Security in Motion“ Teams dazu auf, die eCards und Themen der „my Security & Privacy Box“ im Rahmen von Videoclips zu verfilmen. Durch diesen Wettbewerb, bei dem die Mitarbeiter Inhalte selbst erstellen – das heißt mehr oder weniger eigenständig für die notwendige Awareness bei sich und bei Kolleginnen und Kollegen sorgt –, wird die Selbstverantwortung in Bezug auf Sicherheitsfragen erneut gestärkt – eine der wichtigsten Voraussetzung für wirksame Awareness. ■

Dietmar Pokoyski ist Gründer der Kölner Kommunikationsagentur known_sense. Pokoyski hat 2009 bei vieweg + teubner (edition <kes>) gemeinsam mit Michael Helisch das bis heute einzige deutschsprachige Fachbuch zum Thema Security Awareness herausgegeben.

Interessenten, die den „SECURITY PARCOURS“ live erleben und aktiv mitmachen möchten, haben am 5. Juni 2013 in Köln Gelegenheit dazu. Informationen und Anmeldung unter http://sicherheit.eco.de.

Auszug aus den im Rahmen des „SECURITY PARCOURS“ vermittelten Tipps der „mySecurity & Privacy Box“ zum Thema „Clear Desk“

Arbeitsort aufräumen verhindert Informationen abräumen

Wenn Ihr Arbeitsort kein Büro ist das Sie beim Verlassen abschließen können und eine Vielzahl von Personen (z. B. Kunden) Zutritt hierzu haben, dann kommt dem Prinzip „Need-to-see“ besondere Bedeutung zu. Gleiches gilt für den Schutz vor Gelegenheitsdiebstahl durch „Mitnahme“ unternehmensinterner Werte (z. B. Laptop, Dokumente) aber auch persönlicher Gegenstände der Mitarbeiter (z. B. Geldbörse, Handy).

Wenn Sie Ihren Arbeitsplatz verlassen, sollten Sie …

- … stets Ihren Rechner sperren.
- … keine vertraulichen oder streng vertraulichen Dokumente offen, das heißt ohne Verschluss, liegen lassen.
- … auch keine Notizen von Passwörtern oder anderen Zugangsdaten am Arbeitsplatz liegen lassen.
- … Wertgegenstände immer in einem abgeschlossenen Rollcontainer beziehungsweise Schrank verstauen.
- … Notebooks und gegebenenfalls auch andere elektronische Geräte wie externe Festplatten – mit einem Seil-Schloss (z. B. Kensingtonschloss) oder ähnlichen Hilfsmitteln anketten und so vor Mitnahme schützen.
- … gegebenenfalls (d. h. wenn möglich) Fenster und Türen zusperren.