Anwenderbericht

Security Spot

Awareness- und Risk-Management-Assessment für Manager

Wie schafft man nachhaltige Security-Awareness in der wichtigen Zielgruppe des Managements? T-Systems International nutzt hierzu das das Planspiel „Security Spot", das gleichermaßen Sensibilisierungsinstrument und Risk-Management-Assessment darstellt.

Von Christoph Schog, ##ORT, und Dietmar Pokoyski. ##ORT

Ausgehend von dem Anspruch, Führung nicht mehr länger über rein hierarchische Aspekte wie Position oder etwa Wissensvorsprung zu definieren, sondern als beabsichtigten Beeinflussungsprozess, der vor allem soziale Dimensionen umfasst, repräsentiert ein Manager ein sprichwörtlich ideales Security-Vorbild. Hierzu sollte er unter anderem Security-Awareness-Maßnahmen steuern, aber zum Beispiel auch bei der Abwehr von Risiken dem Social-Engineer ein Schnippchen schlagen, indem er mehr Anerkennung und soziale Teilhabe an sein Team verteilt als ein (oberfläch betrachtet) „netterer" Cyber-Eindringling.

Schaut man sich jedoch die Benchmarks an, die T-Systems seit 2005 über die interne Evaluation von Sensibilisierung – die so genannte „Online-Awareness-Umfrage" (OAU) – generiert, ergibt sich eine ganz andere, fast schon paradox anmutende Wirklichkeit: Der Security-Awareness-Index (S.A.I.) besteht aus den fünf Dimensionen Eigenverantwortlichkeit, Einfluss auf die Aufgabenbewältigung, Sicherheitskultur, Managemenent-Attention und Einstellung zur Sicherheit. Der S.A.I. hat sich bei T-Systems in fast allen Units in den letzten 12 Jahren permanent verbessert – leider nicht überall.

Wenn man bei den Ausnahmen detailliert nachfasst, haben exakt diejenigen Einheiten besonderen Nachholbedarf an genereller Awareness, deren Werte speziell in Bezug auf die „Management Attention" nicht sonderlich positiv auffallen. Dies ist ein eindeutiger Beleg dafür, dass sich Mitarbeiter am Verhalten ihrer Führungskräfte orientieren und eine implizite Anforderung an mehr beziehungsweise bessere zielgruppenspezifische Awareness-Maßnahmen für Manager.

Zwar hat T-Systems diesbezüglich bereits 2010 mit dem Moderations-Tool „mySecurity & Privacy Box" explizit ein Sensibilisierungsinstrument für die Implementierung teambasierter Awareness über die Zielgruppe der Team-Leads generiert – dennoch wurden unbestritten mehr Maßnahmen für „Normalos" durchgeführt. Außerdem hat sich die Awareness in den letzten Jahren deutlich von klassischen Instrumenten der Lerntheorie und typischen Marketingtools hin zu zunehmend systemischen Instrumenten, etwa Simulationen und weiteren Ansätze aus dem Gamification-Umfeld, entwickelt. Solche Maßnahmen drohten, Führungskräfte „abzuhängen", die klassischerweise eher kognitiv ticken und seltener bereit sind, spielerische Ansätze als zielführende Change-Tools zu akzeptieren oder gar zu nutzen.

Trick 17

Aus diesem Grund waren bei der Kreation eines neuen Planspiels für die Zielgruppe „Management" bei T-Systems 2014 zahlreiche Anforderungen zu beachten – die wichtigste: das Thema Awareness durfte die geplante Simulation nicht als Cover-Story tragen, sondern sollte dort nur implizit, als so genannte Impact-Story, untergebracht sein. Praktisch bedeutet dies, dass T-Systems den „Security Spot" als ein klassisches Management-Thema im Rahmen eines Risk-Assessment der besonderen Art vorstellt, das im Rahmen von ISO-27001-Audits auch als aktives Engagement zum Thema Informationssicherheit dargestellt werden kann.

Security-Spot-Cover-Story

_____ Risk-Assessment für Management-Boards und weitere Führungskräfte

_____ Erstellung einer Entscheidungsvorlage, basierend auf den evaluierten Top-Risiken
_____ Erstellung eines Reports mit Maßnahmenkatalog im Nachgang
_____ Implementierung der Folge-Maßnahmen mit Board-Unterstützung (Sponsorship)

Security-Spot-Impact-Story
_____ Steigerung der Security-Awareness von Board-Members
_____ Austausch beziehungsweise Mediation zwischen Security-Professionals und Managern
_____ interner Risiko-Benchmark
_____ Klärung von Rollen und Positionen
_____ Evaluation des Bedarfs hinsichtlich Security-Kommunikation- und Awareness-Maßnahmen
_____ Kreation von bildstarken und lebendigen Security-Lernkarten

Erst in der Impact-Story geht es also beim „Security Spot" um die Security-Awareness der teilnehmenden Manager – außerdem darum, Management-Board und lokales Security-Management in einen gemeinsamen Austausch über Sicherheit im Allgemeinen und Bedrohungen im Besonderen zu involvieren: Denn wann erhalten Security-Manager schon mal anderthalb Stunden Zeit, um konzentriert mit ihrem gesamten Top-Management über Informationssicherheit zu diskutieren? Diese implizite Intention des „Security Spots" wird aber während der Planungsphase eines Spots ausschließlich mit dem lokalen Security-Management erörtert.

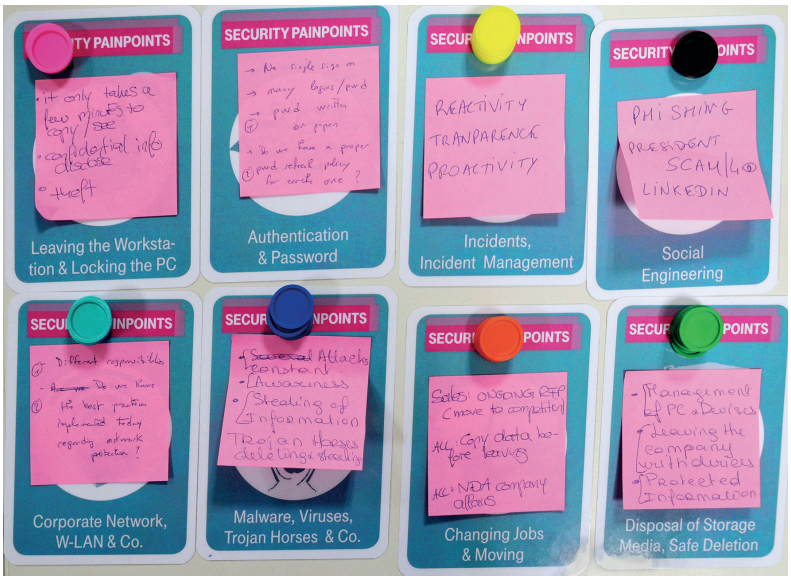
Ablauf

Der „Security Spot" ist ein anderthalb bis zweistündiger „Deep-Dive"-Workshop, der von T-Systems in Kooperation mit dem Awareness-Dienstleister known_sense entwickelt wurde. Als Basis dient das von known_sense gemeinsam mit Marcus Beyer (DXC Technology, vormals HPE) kreierte Moderationskartenset „askitMeta", das außerhalb von T-Systems auch bei Bosch, der BAköV oder der BMW Group eingesetzt wird.

Management-Board beim Planspiel „Security Spot" (T-Systems Malaysia 2016)

Beim „Security Spot" kommen nach einer Vorbereitung durch das zentrale Security-Management (vgl. Kasten zur Dramaturgie) für 90 bis 120 Minuten lokale Sicherheits-Professionals und Board Member von T-Systems zusammen, die ein gemeinsames kommunikatives Verständnis über Informationssicherheit, Risiken und Sensibilisierung anstreben. Dabei werden mithilfe von Planspielkarten, Jetons, einem Spielfeld und einem eindeutigem Regelwerk (alles konfektioniert in einem Planspielkoffer) Risiken und Probleme der Informationssicherheit priorisiert, visualisiert und in Entscheidungshilfen übersetzt. Außerdem lassen sich unter anderem Abwehr-Strategien identifizieren und einheitliche Perspektiven mit klaren Prozessschritten, Meilensteinen sowie einer Übernahme von Sponsorships durch die Manager schaffen.

Als „Big Picture" ordnen die Teilnehmer am Ende die von ihnen ausgewählten (priorisierten) Security-"Painpoints" einem individuellem, im Rahmen eines Vorbereitungs-Workshops erstellten



Security-Spot-Karten nach der letzten Priorisierung (beispielhafte Auswahl)

Business-Steckbrief der jeweiligen Unit auf einem Spielfeld zu, wodurch die Auswirkungen von Risiken auf das Geschäft visualisiert werden. Dies funktioniert im Grunde genommen ähnlich wie eine Mischung aus Poker und Roulette, nur dass hier der Zufall völlig außen vor bleibt und jede Aktion einer bewussten oder zunächst unbewussten (aber im Nachgang stets nachvollziehbaren) Entscheidung zugrunde liegt.

Für jede Zuordnung soll idealerweise ein Sponsor gefunden werden: das heißt, dass die Teilnehmer sich bei Handlungsbedarf in einem der identifizierten Felder als Ansprech- oder Sparringspartner des lokalen Security-Managements zur Verfügung stellen.

Nach Abschluss des Planspiels wird ein Report mit beispielhaften Bildern aus dem Workshop sowie einer Beschreibung der Workshop-Atmosphäre inklusive Benchmarks zu weiteren, bereits vorliegenden Risk-Assessments und Audits beziehungsweise Ergebnissen und Empfehlungen für Folgemaßnahmen erstellt und dem Management als Entscheidungsvorlage präsentiert.

Security-Spot-Dramaturgie im Überblick

_____ Bis zu 6 Wochen vor dem Spot: Vorbereitung via regelmäßiger Telefonkonferenzen mit dem lokalen Security-Management

_____ Einen Tag vor dem Spot: Vorbereitungs-Workshop mit dem lokalen Security-Management – unter anderem Ausfüllen des Security-Spot-Spielfelds

_____ „Security Spot“ mit maximal 14 Teilnehmern: Auswahl von Sicherheits-Bildkarten für die Vorstellungsrunde

_____ 2–3 Priorisierungsrunden bei den Security-Painpoint-Karten mit Vorstellung der Gründe für die jeweilige Auswahl durch die Teilnehmer

_____ Platzierung farbiger Jetons als Stellvertreter der Sicherheitsrisiken auf die finale Auswahl von 6–12 Security-Painpoint-Karten

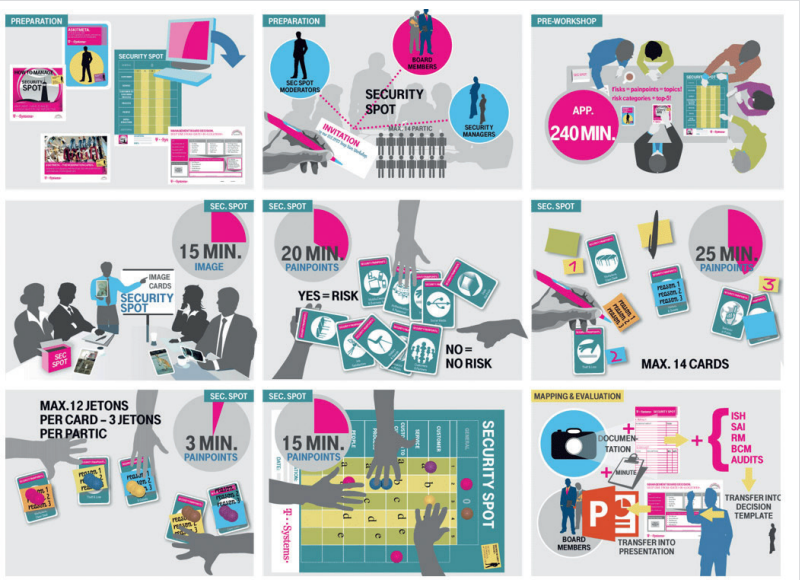
_____ Aufklappen des Spielfelds mit dem Business-Framework der jeweiligen Unit und finale Auswahl von 2–3 Risiken (Jetons) durch jeden Teilnehmer mit anschließender Positionierung auf dem Spielfeld (Zuordnung von Risiken auf diejenigen neuralgischen Business-Felder, bei denen die Painpoints konkrete Wirkung auf das Geschäft ausüben)

_____ Schlussrunde mit Begründung der Positionierung, Fazit und Übernahme von Sponsorships durch Board-Member

_____ Etwa 2–3 Wochen nach dem Spot: Evaluation mit Erstellung von Report und Evaluationsposter als Key-Visual („Big Picture“) des Workshops sowie Maßnahmenkatalog

_____ Anschließend: Präsentation des Reports vor dem Management-Board durch das lokale Security-Management mit Beschlüssen hinsichtlich der vorgeschlagenen Maßnahmen

_____ Im Nachgang regelmäßiger Austausch zwischen Security-Management und Sponsoren



Skizze der Phasen im „Deep-Dive“-Prozess

Erfahrungen und Ergebnisse

Jede T-Systems-Einheit kann ihren eigenen „Security Spot“ organisieren: Durchgeführt wurde dieser in den letzten zwei Jahren bereits in Deutschland, in der Schweiz, in Belgien, Frankreich, Malaysia und Singapur – bisher stets mit Erfolg, da über den Workshop in jedem dieser internationalen Units die vermeintlichen Differenzen zwischen der klassischen Businesssicht des Boards und den vom Security-Management erstrebten Abwehr-Bedarf deutlich verringert werden konnten.

Anhand eines Reports und Evaluations-Posters wird der Status quo jeder Unit mit dem jeweiligen Handlungsbedarf beschreiben und visualisiert. Anhand der ausgewählten Painpoints (in Form von Bildkarten, siehe Kasten) lässt sich zudem auch ein Wirkungsgefüge der lokalen Sicherheitskultur evaluieren.

Die meisten „Security Spots“ haben Ergebnisse aus vorherigen Risk-Assessments der jeweiligen Unit bestätigt. Jedoch kam es in fast allen Fällen auch zu neuen, teilweise überraschenden Resultaten: Diese betrafen überwiegend mangelnde oder fehlerhafte Security-Kommunikation, etwa eine unzureichende kommunikative Begleitung bei der

Einführung neuer Prozesse oder Tools oder schlichtweg fehlende respektive nicht zu Ende gedachte Security-Awareness-Maßnahmen.

Mithilfe der Spots konnten potenziell zielführende Maßnahmen definiert und auf Basis der Kooperation von lokalem Security-Management und den Sponsoren aus dem Board implementiert werden. In einigen der Standorte wurden so erfolgreiche Awarenessformate „auf Strecke gebracht" – etwa der „Security Parcours", eine spielbasierte, mehrfach ausgezeichnete Lernstations-Roadshow, oder die laufende Aktion „Card of the Month", eine Promotion-Strecke für die themenorientierten Moderationskarten der bereits erwähnten „mySecurity & Privacy Box".

In einem Fall wurde im Verlauf des Workshops der zunehmende Widerstand des gesamten Management-Boards gegenüber Sicherheitsmaßnahmen gewahr: Kein Zufall, denn hierbei handelte es sich ausgerechnet um diejenige Unit, die in der Online-Awareness-Umfrage (OAU) in Bezug auf die Dimension „Management-Attention" die rote Laterne innehatte.

Die Herausarbeitung derartiger oder ähnlicher Zusammenhänge unterstützt das Security-Management dabei, sein Handeln, einzuführende Prozesse, Tools oder Maßnahmen gegenüber den Business-Entscheidern zu begründen. Das bedeutet letztlich, dass Security-Management dann nicht nur im „luftleeren Raum" oder auf dem Papier stattfindet, sondern vielmehr im Kontext einer fassbaren und tatsächlich auch beschreibbaren Sicherheitskultur.

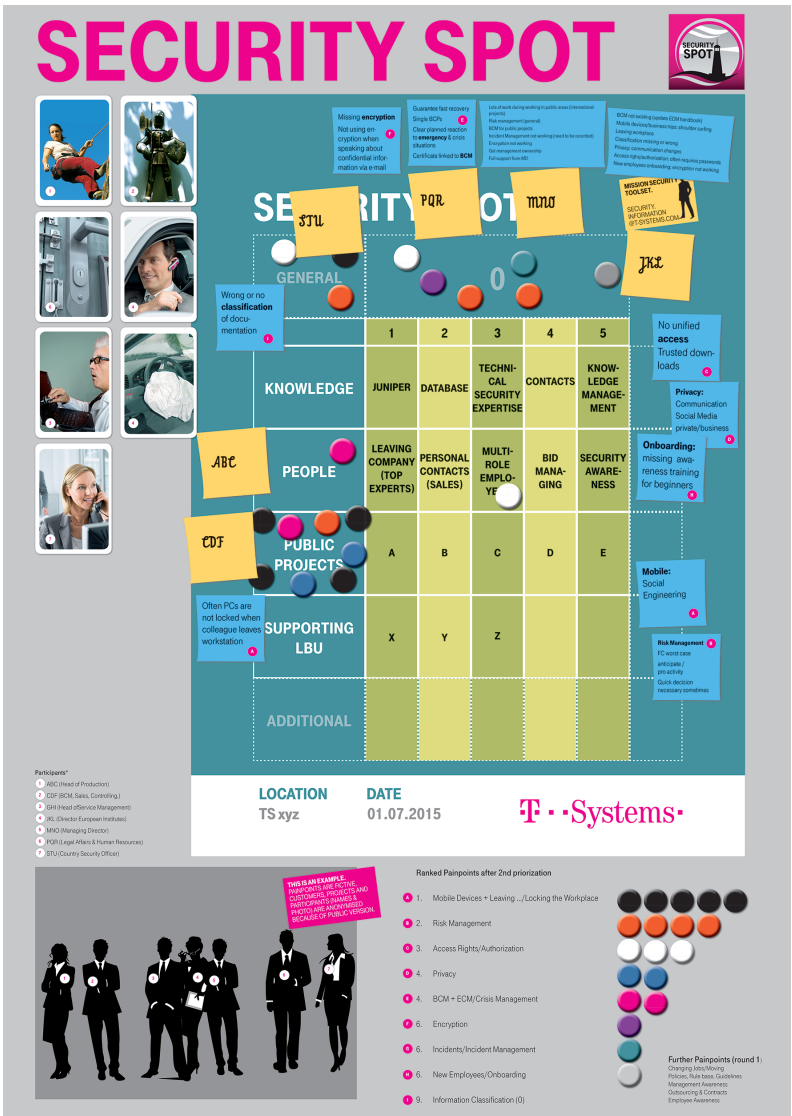
Fazit

Sicherheit – so zeigt es auch der Spot – ist ein Kommunikationsthema! Oft trägt ein Verschieben der Perspektive oder eine Klärung des „offiziell Gemeinten" (aber manchmal Unausgesprochenem) jenseits einer oberflächtlichen, kognitiven Kommunikationsebene dazu bei, dass Security-Management und Management-Boards hinsichtlich ihren Einschätzungen gar nicht mal so weit auseinander liegen.

Auch das kann letztlich „Security by Design" sein: Ein spielerischer Umgang, der auch die nonverbale, visuelle Ebene und implizite Kommunikation mit der Beteiligung sämtlicher Sinne (regelbasiert) integriert, ist am Ende gegenüber der reinen, verbalen oder schriftlichen Verhandlungsebene klar im Vorteil – gerade gegenüber stark prozessorientierten, vordergründig IT-lastigen Risiko-Szenarien wie etwa COBIT oder IRAM2. ■

Dr. Christoph Schog ist als Security Manager bei T-Systems unter anderem zuständig für Security-Awareness. Dietmar Pokoyski ist Geschäftsführer von known_sense, einer Kommunikations- und Beratungsagentur mit Fokus auf interne Kommunikation und Awareness – besonders für Sicherheits- und Datenschutzthemen.

Im Rahmen einer Roadshow bieten T-Systems und known_sense ab November Unternehmen in Berlin, Köln, Frankfurt/Main und Münschen an, den „Security Spot" einmal live auszuprobieren (Dauer ca. 90 Minuten) – bei Interesse schreiben Sie bitte an pokoyski@known-sense.de. Der „Security Spot" wird zudem auch beim 28. Annual ISF World Congress vom 28.–31. Oktober 2017 in Cannes (FR) als Best-Practice-Tool präsentiert.



Security-Spot-Evaluations-Poster (anonymisiertes Beispiel)