Security-Awareness-Programm unter Berücksichtigung viraler Marketingmethoden

Kirsten Brox, Anastasia Meletiadou
Unternehmenssicherheit und Compliance
buw Holding GmbH
Rheiner Landstraße 195
49078 Osnabrück
kirsten.brox@buw.de
anastasia.meletiadou@buw.de

Abstract: In diesem Beitrag wird ein Programm zur effektiven Sicherheitssensibilisierung im Unternehmen entwickelt. Schwerpunkte des Programms liegen auf Bedrohungsszenarien, der Form eines ‚Alternate Reality Game' zur Wissensvermittlung und messbaren Erfolgsgrößen. Mithilfe des Programms soll eine dauerhafte Verhaltensänderung erreicht werden.

1 Zielsetzung

Unwissenheit und mangelndes Verantwortungsbewusstsein in Bezug auf Informationssicherheit führen zu erheblichen Problemen für Unternehmen und Behörden. Die sicherste Informationstechnik kann ihren Schutz nicht entfalten, wenn Mitarbeiter mit den überlassenen Informationen fahrlässig agieren. In den vergangenen Jahren haben Studien wiederholt gezeigt, dass eine der größten Schwachstellen in der Informationssicherheit der Mensch ist: Mitarbeiter die Kennungen weitergeben, sich nicht gut über Informationssicherheit informiert fühlen oder den Wert ihres Unternehmenskennworts unterschätzen [Ros12] [Fon12] [DGHA12].

Zudem gibt es Bereiche, in denen Informationssicherheit nicht ausreichend oder nicht wirtschaftlich durch technische Lösungen erreicht werden kann. Beispiele sind etwa der Schutz vor Phishing-Angriffen oder einer gezielten Ansprache von Mitarbeitern, um sie zur Preisgabe vertraulicher Informationen zu bewegen. Es ist anzunehmen, dass mit erhöhtem Aufkommen von Angriffen auch die Zahl der erfolgreichen Versuche ansteigt. Deshalb ist es nicht verwunderlich, dass beispielsweise die Zahl der versuchten Phishing-Angriffe von 2011 bis 2013 um 87% zugenommen hat [ZAO13].

Die beiden zentralen Elemente von Awareness-Programmen sind sowohl den Mitarbeitern die erforderlichen Wissensinhalte zu vermitteln, als auch den inneren bzw. äußeren Anreiz zu schaffen, dieses Wissen anzuwenden. Im Rahmen dieses Beitrags wird Security-Awareness als ein Gesamtprogramm von Sensibilisierungselementen zur nachhaltigen Verhaltensänderung definiert. Ziele sind:

1. Mitarbeiter sollen notwendige Sicherheitsmaßnahmen und Regeln als sinnvoll erkennen und positiv besetzen. Angestrebt wird eine Einstellungsänderung vom ‚Regeln einhalten müssen' hin zum ‚Vorbeugen können'.
2. Es ist darauf zu achten, dass Maßnahmen unternehmenskulturell passend implementiert werden und von den Rezipienten nicht als Fremdkörper empfunden werden.
3. Initiierung eines Dialogs zwischen dem Informationssicherheitsmanagement und den Kollegen, die bisher passiv die Regeln anwenden mussten. Methodisch fundierte und erprobte Ansätze sollen die Basis für die Maßnahmen bilden.
4. Es sollen möglichst innovative werbliche Möglichkeiten ausgeschöpft werden, um den Erfolg zu gewährleisten. Das Programm soll für das Qualitätsmanagement Ansätze zur Ermittlung von Kennzahlen und Erfolgsquoten beinhalten.

2 Grundlagen

Im vorliegenden Abschnitt wird die Fragestellung beleuchtet, welche Faktoren bei einem Security-Awareness-Programm zu berücksichtigen sind. Darauf aufbauend wird in Abschnitt 3 ein Framework entwickelt, das als Grundlage für Awareness-Programme in einer Vielzahl von Institutionen dienen kann. Die Umsetzbarkeit (Abschnitt 4) und Wirksamkeit (Abschnitt 5) wurden schließlich exemplarisch mithilfe der Umsetzung des Programms in der buw Unternehmensgruppe überprüft.

2.1 Motivation schaffen

Einen Ansatz menschliches Verhalten zu beeinflussen, liefert das Elaboration Likelihood Model (vgl. Abbildung 1) [Pet86]. Es beschreibt die Auswirkungen einer Mitteilung auf den Empfänger hinsichtlich seiner Einstellung gegenüber dem Thema der Mitteilung. Nach diesem Prinzip können und werden Personen am besten Informationen verarbeiten und in neues Verhalten umsetzen, für die sie eine hohe Motivation haben und deshalb eine Aufnahmebereitschaft besitzen [Hal98] [EKR08] [PTZ13].

Personen setzen sich auf der sogenannten ‚zentralen Route' kritisch mit der Information auseinander. Daraus resultiert eine Verhaltensänderung und eine neue änderungsresistente Einstellung. Bei fehlender Motivation werden die Informationen auf der ‚peripheren Route' hingegen nur oberflächlich untersucht und führen, wenn überhaupt, zu einer instabilen Einstellungsänderung. Häufig werden diese ungewollten Informationen sogar als störend empfunden und führen zu einer Abneigung gegenüber dem betreffenden Thema oder sogar gegenüber dem Mitteilenden.

Für die gewünschte Einstellungsänderung wird demzufolge Motivation benötigt. Der Anreiz muss so hoch sein, dass er mögliche Unbequemlichkeiten überwiegt. Bezogen auf Security-Awareness ist deshalb Motivation im Sinne eines Wachrüttelns eine tragende Säule.

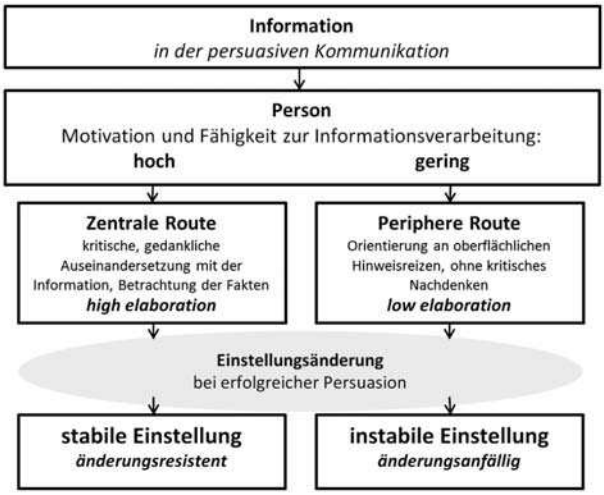

Abbildung 1: Elaboration Likelihood Model [Pet86]

2.2 Wissen vermitteln

Der Sicht von Awareness als wortgetreue Übersetzung, nämlich das Sicherheitsbewusstsein der Mitarbeiter, welches es zu verändern gilt, liegt häufig die Annahme zugrunde, dass die bewusste Einstellung eindeutig mit sicherheitskonformem Verhalten korreliert [Mat09] [mOTG13] [AG13a] [HP09]. Dabei bleibt unberücksichtigt, dass das Bewusstsein über einen Sachverhalt nicht dessen Verständnis impliziert.

Für den Erfolg von Wissensvermittlungen spielen zwei Faktoren eine wesentliche Rolle. Zunächst die Frage, wie gut der Lernstoff vermittelt und verstanden wird. Im Zusammenhang mit Security-Awareness gelingt es in der Regel, die komplexen Themen auf einfache Lerninhalte für die Zielgruppe zu reduzieren. So ist es für den Anwender beispielsweise nicht notwendig etwas über dynamische Schlüssel, das Temporal Key Integrity Protocol (TKIP), Pre-shared keys (PSK) oder Extensible Authentication Protocol (EAP) zu wissen. Zur sicheren Benutzung eines Funknetzes genügt die Information, dass WPA2 gegenüber WEP zu bevorzugen ist [SWA05].

Der zweite und wesentliche Faktor ist der Zeitraum, über den der Lernende diesen Stoff behalten kann. Die Psychologie ist dahingehend gut erforscht und es ist gemeinhin bekannt, wie lange der Mensch neu Gelerntes behält. Der Vorgang des Vergessens kann demnach durch mehrfaches Wiederholen des Lernstoffes abgemindert werden (Überlernen), jede Wiederholung vergrößert das Intervall, nach dem eine erneute Wiederholung notwendig ist [MN90]. Daraus resultiert die Notwendigkeit, ein Awareness-Programm und insbesondere die damit verbundene Wissensvermittlung über einen längeren Zeitraum zu strecken, sodass das Thema in Abständen immer wieder in den Fokus rückt und langfristig Wirkung entfalten kann [cA13].

2.3 Emotionen wecken

Bei der Reduktion von Awareness auf zusätzliche Schulungsmaßnahmen [Rup13] [Inc13] [aG13b], bleibt vielfach unberücksichtigt, dass das neu erworbene Wissen nicht notwendigerweise zu verändertem Verhalten führt.

In der unternehmensinternen Kommunikation konkurriert Informationssicherheit mit einer Vielzahl weiterer, wichtiger Themen wie Mitarbeiterführung, Kundenbetreuung oder Abwicklung des Tagesgeschäfts. Deshalb ist es erforderlich, Sicherheit systematisch im Unternehmen zu vermarkten, damit sie als Top-Thema wahrgenommen wird. Als zusätzliche Herausforderung ruft Sicherheit in der Ausgangssituation eher unangenehme Gefühle hervor. Sie wird mit zusätzlicher Arbeit, Komfortverzicht oder als Freiheitseinschränkung assoziiert.

Im Sinne der Zielerreichung muss Sicherheit positiv besetzt werden und ein akzeptiertes Verhalten sein. Bei der Suche nach möglichst innovativen Kommunikationsformen, fällt vor allem das virale Marketing als geeigneter Kandidat ins Auge. „Virales Marketing beschreibt das gezielte Auslösen von Mundpropaganda zum Zwecke der Vermarktung von Unternehmen und deren Leistungen [Lan09].“ In Anlehnung an den medizinischen Begriff des Virus soll sich dabei die Information über ein Produkt oder eine Dienstleistung epidemisch von Mensch zu Mensch verbreiten, sodass sich das Interesse am beworbenen Produkt und damit dessen Bekanntheitsgrad erhöhen. Diese Vorgehensweise fördert zudem den erwünschten Dialog.

Virales Marketing erzielt durch Emotionalität teilweise beeindruckende Erfolge. Als aktuelles Beispiel für erfolgreiches virales Marketing sei hier ein Projekt des Unternehmens Blendtec vorgestellt: Blendtec, ein Hersteller für Küchengeräte, rief einen Youtube Kanal ins Leben, in dem ein Küchenmixer dazu verwendet wird, Gegenstände zu zerstören. Die Reichweite ist erstaunlich. So wurde die Folge, in der ein i-Pad zerstört wird über 16 Millionen Mal gesehen und fast 50.000 Mal kommentiert [Ble13b]. Laut einer Aussage der Unternehmensführung von Blendtec steigerten sich die Verkäufe nach Einführung der Show um 700% [Ble13a].

Die Vorgehensweise lässt sich auf die Vermarktung von Sicherheit übertragen. Im ersten Schritt erfolgt das sogenannte ‚Seeding‘ (engl. für Impfen oder Aussäen). Mithilfe einer kreativen Idee wird der Inhalt an einer Stelle im Interessentenumfeld platziert. Von dort soll er sich selbständig mit steigender Popularität verbreiten.

3 Framework

Es existieren bereits erprobte Modelle für Security-Awareness-Frameworks. Diese setzen ihren Schwerpunkt z. B. auf den Lebenszyklus eines Mitarbeiters im Unternehmen [Sch13], die starke Einbeziehung der jeweiligen Fachabteilung [KS13] und den Einsatz moderner Medien mit Comics und Web 2.0 Elementen [ED13]. Aus den Grundlagen der vorigen Ausführungen und nach Sichtung bekannter Frameworks wurde für das Programm die Vorgehensweise in Abbildung 2 abgeleitet.

Abbildung 2: Framework für Awareness-Programm [eigene Abbildung]

In einem ersten Initialisierungsprozess gilt es ein geeignetes Thema zu identifizieren und Zielgruppen des Programms festzulegen. Bei der Wahl des Themas sollten die folgenden Faktoren berücksichtigt werden: Wahrscheinlichkeit des Eintretens, Höhe des Schadens, Einflussnahme durch Verhalten der Mitarbeiter. Bereits in dieser Phase ist es unabdingbar die Unternehmensleitung einzubeziehen, da sie nicht nur notwendige Freigaben für die Planung erteilen muss, sondern auch auf die Ausrichtung des Programms strategischen Einfluss nehmen sollte.

In Anlehnung an das gewählte Thema muss ein glaubwürdiges Szenario für die Anwender entwickelt werden. Das Risiko soll erlebbar gemacht werden, in der Regel durch eine Angriffssimulation. Die BSI Studie „Durchführungskonzept für Penetrationstests“ [fSidI03] beschreibt als Vorgehensweise zunächst das Angriffsziel zu definieren und ein Konzept festzulegen. Bei der Konzeptionierung muss an die möglicherweise nötigen Verträge wie z. B. Geheimhaltungsvereinbarung genauso gedacht werden, wie an die Einbeziehung aller wichtigen Beteiligten, wie Betriebsrat oder Datenschutzbeauftragte. Bei der Durchführung sollen Mitarbeiter keinesfalls durch dauernde Wiederholung der Simulationen negative Assoziation erfahren. In der Abschlussanalyse zeigt sich dann, ob die Risiken während der Initialisierung richtig gewählt wurden. Denn nun lässt sich messen, ob von den angenommenen Risiken echte Bedrohungen ausgehen und ob die Anwender durch ihr Verhalten die Gefährdung wirksam abgewendet haben.

Aus der Abschlussanalyse resultieren die Lernziele für die Wissensvermittlung, es sind genau jene Punkte, in denen die Mitarbeiter durch ihr Verhalten ein Risiko für die Informationssicherheit provoziert haben. Für diese Ziele wird eine Lehrmethode gewählt, ein Lehrplan für jede Zielgruppe erstellt und umgesetzt. Dabei sind die positive Vermarktung des Themas und die emotionale Aufladung zu berücksichtigen. Am Ende dieser Phase ist eine weitere Analyse empfehlenswert, um den Wirkungsgrad des Schulungskonzepts zu

bewerten.

Zur Sicherung der Nachhaltigkeit werden die Ergebnisse der Unternehmensleitung präsentiert und für alle Mitarbeiter aufbereitet. Dabei ist die Wahl der Kommunikationsmethode ebenso entscheidend, wie bei der Wissensvermittlung selbst. In einer Analyse sind Verbesserungen für zukünftige Programme zu ermitteln, bevor zu einer neuen Initialisierung übergeleitet werden kann.

4 Praxisbeispiel

Die buw Unternehmensgruppe ist im Bereich Customer Care tätig und unterliegt somit als Auftragsdatenverarbeiter verschiedenen vertraglichen und gesetzlichen Anforderungen nach §11 Bundesdatenschutzgesetz (BDSG). Um die notwendige sicherheitsbewusste Kultur zu etablieren, verfolgt das Unternehmen bereits mehrere Ansätze. Es wurde ein ISMS (InformationsSicherheitsManagementSystem) installiert und nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert. Auf Grundlage einer unternehmensinternen Sicherheitsrichtlinie „Sensibilisierung und Schulung zur Informationssicherheit“ werden bereits eine Reihe von Sensibilisierungsmaßnahmen durchgeführt. Trotz dieser umfangreichen Vorkehrungen lassen sich Sicherheitsvorfälle auf ungenügendes Wissen oder die Nicht-Einhaltung von Sicherheitsmaßnahmen zurückführen.

4.1 Initialisierung

Basierend auf dem Framework (vgl. Abbildung 2) wurde in der buw Unternehmensgruppe zunächst das Thema festgelegt. Verglichen wurden Risiken im Umgang mit Informationen, wie beispielsweise Wirtschaftsspionage, Sabotage, Datenmanipulation und Datendiebstahl. Als Ergebnis des Vergleichs wurde der Bereich Datendiebstahl als erfolgversprechendstes Thema für das Programm identifiziert. Die Wahrscheinlichkeit eines Verlusts vertraulicher Daten an einen externen Angreifer wäre durch die Vielzahl der Möglichkeiten hoch, der Schaden wäre beträchtlich und korrektes Verhalten der Mitarbeiter wäre eine wirksame Gegenmaßnahme.

Die Zielgruppe wurde auf alle 5.000 Mitarbeiter an 10 Standorten der Unternehmensgruppe festgelegt. Jedoch sollte der Schwerpunkt auf dem deutlich kleineren Anteil der Anwender liegen, die Funktechnologie, einen E-Mail-Account und das Internet verwenden. Dort wurde ein erhöhtes Risiko für Datendiebstahl vermutet. Der zeitliche Rahmen wurde auf 4 Monate angelegt, so dass ausreichend Zeit für die nötige Wissensvermittlung zur Verfügung stand. Zur Kennzahlermittlung wurden die Kriterien Gesamtzahl der Angriffe, Zahl der erfolgreichen Angriffe und die Vertraulichkeitsklasse der entwendeten Informationen betrachtet. Um die Kampagne intern zu präsentieren, konnte auf die Unterstützung des Fachbereichs Marketing zurückgegriffen werden. Daraus resultierte die Gestaltung eines Kampagnenlogos mit einem stilisierten Banditenkopf und das Motto „Bis jetzt ist ja auch nichts passiert. Bis jetzt“. Dem Thema folgend wurden in der Motivationsphase sämtli-

che mit dem Programm zusammenhängende Aktionen mit dem Angriff eines virtuellen Banditen verknüpft. Firmenkulturell waren Benchmarks der Standorte oder Abteilungen gegeneinander bereits etabliert. Im Zuge des Programms wurde diesem bekannten Vorgehen der gemeinsame Feind in Form des Banditen hinzugefügt. Es sollte ein Wettbewerb von Abteilungen sein, mit dem Ziel den Banditen zu besiegen.

4.2 Motivation

Das Szenario bestand aus einem Außentäter, der versuchen sollte, vertrauliche Daten zu stehlen. Dabei wurde die Art eines Blackbox-Tests gewählt. Der extern beauftragte Angreifer erhielt im Vorfeld keine Informationen über das Unternehmen. Nach Abschluss eines Geheimhaltungsvertrags und Rücksprache mit den Datenschutzbeauftragen wurde die Aufgabenstellung formuliert. Das Vorgehen sollte vorsichtig abwägend und eher laienhaft sein. Die interne Erwartungshaltung war deshalb ein Fehlschlagen des Datendiebstahls in allen 5 konkreten Arbeitsaufträgen:

1. Simulierter Telefonangriff: Der Externe rief in unterschiedlichen Unternehmensbereichen an und versuchte sensible Informationen zu erfragen.
2. Unberechtigter Zutritt: Er versuchte sich während der Bürozeiten unberechtigt Zutritt zum Gebäude verschaffen. Dort sammelte er Dokumente und hielt nach ungesperrten Rechnern, unbeaufsichtigten Mobiltelefonen oder mobilen Datenträgern Ausschau.
3. Phishing: Eine E-Mail mit einem Phishing-Link von einer als intern getarnten, jedoch nicht existenten E-Mailadresse und mit deutlichen Auffälligkeiten in der Ansprache wurde an alle Mitarbeiter gesendet. Beim Klick auf den Link, landete der Empfänger auf einem Eingabedialog, optisch ähnlich dem Exchange Webmail. Wenn er dort einen Loginversuch startete, landete er auf einer Sensibilisierungswebseite, die ihn über Phishing aufklärte.
4. Präparierte Speichermedien auf dem Firmengelände: Auf ausgelegten USB-Sticks lag eine Datei ‚[Filmtitel].mp4.exe‘. Wurde sie auf einem Unternehmensrechner ausgeführt, erfasste sie den lokalen Rechnernamen und produzierte ein Warnfenster mit dem Kampagnenmotto.
5. WLAN-Honeypot: Ein präparierter WLAN-Router wurde aufgestellt. Bei Verbindung erschien eine html-Seite mit Logindialog.

Zu jedem Arbeitsauftrag wurde eine konkrete Auswertung der Menge der Ziele und der Menge und Art der gestohlenen Daten ermittelt. Dabei wurde bewusst auf eine personenscharfe Analyse verzichtet. Die Abschlussanalyse ist nicht öffentlich, entgegen der oben erwähnten Erwartungshaltung wurden jedoch bei allen Aufträgen Schwachstellen mit Datenverlust verzeichnet. Das Thema und die Angriffsszenarien wurden demnach richtig gewählt.

Den Abschluss der Motivationsphase bildete eine Präsentation für die Geschäftsführung mit den konkreten Ergebnissen, sowie eine Informationsmail an alle Mitarbeiter. Letztere wurde im Namen des Banditen in Form einer ‚Kriegserklärung' verschickt und war gleichzeitig Auftakt zur Wissensvermittlung.

4.3 Wissen vermitteln

Die ermittelten Schwächen wurden dazu verwendet, passgenau das fehlende Wissen zu identifizieren. Alle Mitarbeiter sollten über die Angriffe informiert und mit Kenntnissen ausgestattet werden, wie die aufgetretenen Fehler in Zukunft konkret vermieden werden können. Ziel war explizit nicht nur die Präsentation vorgefertigter Wissensfragmente, sondern der selbständige Umgang mit Informationssicherheit und die Einbettung der Wissensvermittlung in den Arbeitsalltag.

Zur Lehrmethode wurden unterschiedliche Strategien verglichen. Gegen die Präsenzschulung sprachen die räumliche Distanz der zehn Standorte des Unternehmens, das unterschiedliche Vorwissen der Mitarbeiter, wie auch das nicht individualisierbare Lerntempo. Zudem sollte sich das Programm deutlich von den bereits regelmäßig zu absolvierenden Schulungen zur Informationssicherheit, aber auch fachlichen Themen, abgrenzen. Um möglichst viele oder sogar alle Mitarbeiter des Unternehmens zu erreichen, wären 250 Schulungstermine notwendig gewesen – eine organisatorische Unmöglichkeit im Programmzeitraum.

Der technische Aufwand einer Implementierung über alle Standorte und die Einweisung aller Organisatoren wäre bei einem e-Learning mit immensem Aufwand verbunden und würde hohe Selbstlernkompetenz bei allen Teilnehmern verlangen. Zudem sollten die Lernenden ein Thema, nämlich das Social Engineering, bewerten lernen, bei dem es im Wesentlichen um Kommunikation zwischen Menschen geht. Diesen Inhalt über eine rein technische Plattform zu verteilen, schien unpassend. Zuletzt birgt ein e-Learning ohne Ansprechpartner immer eine erhöhte Gefahr der Missdeutung von Inhalten.

Die Lehrmethode sollte in den Alltag eingebettet sein, zu Aktivität anregen und innovativ die geweckte Neugier aus der vorigen Angriffsituation befriedigen. Die Wahl fiel auf eine Einbettung der Wissensvermittlung in ein Spiel. Verwendete Elemente sollten unter anderem Highscores, Fortschrittsbalken, Ranglisten und Auszeichnungen sein. Datenanalysen zeigen signifikante Verbesserungen in Bereichen wie Benutzermotivation, Lernerfolg, Verhaltensänderung, Lerngeschwindigkeit und Nachhaltigkeit bei deren Verwendung [Cha13]. Bereits 2011 antizipierte eine Gartner Studie, dass ‚Gamifizierung' ein signifikanter Trend sei, den bis 2014 über 70% der Top-2.000-Unternehmen eingebunden haben werden [Por12].

Eine Befragung in einem Unternehmen, das ein ‚Alternate Reality Game', unter anderem zur Spamabwehr absolviert hatte, ergab, dass nach dem Programm 95% der Befragten eine Spam E-Mail korrekt erkennen konnten und alle Befragten an einem weiteren Programm teilnehmen wollten [elT10]. Ein Alternate Reality Game zeichnet sich dadurch aus, dass es die Grenzen zwischen Spiel und Wirklichkeit bewusst verwischt. Die Mitspieler betreten über ein sogenanntes ‚Rabbit Hole', ein unerwartetes Ereignis im Alltag, das Spiel. Die Spielinhalte werden über unterschiedliche Medien in den Alltag verlagert. Diese Methode

schien nach Bewertung der Anforderungen passend für die Wissensvermittlung in der buw Unternehmensgruppe geeignet zu sein. Das Spiel sollte sich nahtlos in den Arbeitsalltag einfügen und die Teilnehmer mit unterschiedlichen Medien für das Thema interessieren. Der Ablauf wurde wie folgt festgelegt.

Level 1

Das Seeding, also die kreative Idee, die ausgesät wurde, war zugleich der Zugang zum Alternate Reality Game: das Rabbit Hole. Per Post bekam jede Abteilung eine Holzkiste mit Geheimfach. Im Geheimfach befand sich ein Logical-Rätsel. Zur Lösung waren Wissen über richtige Verhaltensweisen im Unternehmen, wie auch logisches Denken gefordert. Aus der Lösung des Rätsels ergab sich ein Link zu einer Webseite im Intranet. Diese Kampagnenseite wurde während des gesamten Spiels der Anlaufpunkt für alle Mitspieler. Auf der Webseite befanden sich eine Übersicht aller Standorte und Abteilungen mit Anzahl erfolgreicher Spieler, Link zu einem Wissensquiz, ein Counter bereits gelöster Quizzes, ein Infoticker mit aktuellen Neuigkeiten und ein Chat zur Kontaktaufnahme.

Level 2

Auf der Kampagnenseite erschien ein Hinweis im Ticker, dass Level 2 eröffnet sei. Klicken konnte man dieses Mal allerdings nichts. Zeitgleich erschien der turnusmäßige Datenschutz-Newsletter mit einem unauffälligen Morsecode. Der Code führte auf das zweite Quiz zum Thema mobile Datenträger. Mitarbeiter, die dieses Training absolviert haben, füllten damit den zweiten Counter.

Level 3

Nach einer angemessenen Lernzeit erfolgte auf der Kampagnenseite der Hinweis auf das nächste und letzte Level und ein Hinweis auf die im Unternehmen vorhandene Clean-Desk-Policy. In der darauffolgenden Woche wurden Karten auf den Schreibtischen ausgelegt, auf denen sich neben dem Dank für den aufgeräumten Schreibtisch auch je eine Rechenaufgabe befand. Die Lösung aller Aufgaben ergab eine interne Telefonnummer, unter der der Bandit zum letzten Test mit dem Thema WLAN aufforderte.

4.4 Nachhaltigkeit sichern

Alle Analysen, also sowohl die Angriffsergebnisse, wie auch der Verlauf des Schulungsspiels, wurden zu einer Abschlusspräsentation für die Geschäftsführung zusammengefasst. Die Angriffszenarien und die Merksätze wurden außerdem in Form eines Posters und einer Intranetseite für die Mitarbeiter dauerhaft zugänglich gemacht. Zudem wurde das Programm mit mehreren Beiträgen im Firmenblog und einem Bericht in der Firmenzeitung für Mitarbeiter und Kunden besonders gewürdigt. Auf der Intranetseite fand eine Abschlussbefragung statt, um Reichweite und Eindrücke der Teilnehmer messbar zu machen.

5 Bewertung

Das konzipierte Programm war ein Erfolg. Es konnte im Rahmen des vorgegebenen Frameworks umgesetzt werden. Die Beschäftigung mit Informationssicherheit in spielerischer Form wurde positiv wahrgenommen. In der Befragung gaben 47% an, dass sie gern mitgespielt haben und bei einer Wiederholung erneut mitspielen würden. Im Vergleich dazu äußerten sich nur 3% kritisch und würden bei einer Wiederholung nicht mehr teilnehmen. Es ist zu eruieren, was für Gründe diese Mitspieler für ihre Entscheidung hatten.

Unmittelbar nach Spielbeginn bekam der Fachbereich für Informationssicherheit mehrfach Feedback und gezielte Fragen nach Lösungshinweisen. Exemplarisch sei hier das Zitat einer Mitarbeiter-E-Mail wiedergegeben: „Der sportliche Ehrgeiz ist geweckt! Auch wenn wir am Ende vielleicht nicht die Nase vorn haben sollten – wir haben den Kampf angenommen! Wir rühren jedenfalls mächtig die Werbetrommel und verteilen Quizhefte und vergrößerte Lösungsmatrizen."

Auch konkrete Sicherheitsüberlegungen wurden geschildert und mit den hausinternen Ansprechpartnern diskutiert. Die Mitspieler kamen aktiv auf die Idee Hilfsmittel einzusetzen und beschäftigten sich mit großem Engagement mit der Informationssicherheit. Im Verlauf des Spiels sank der Anteil der falsch beantworteten Quizfragen, ein Hinweis auf den Erfolg der Lernphase. Zudem wurden aus der Angriffsphase wertvolle Erkenntnisse über Prozesschwächen und Risiken gewonnen.

Viralität

Das Spiel wurde mit 77 Holzkisten initiiert. Am Ende des ersten Levels waren bereits über 700 Quiz gelöst. Neben dem persönlichen Austausch mit Kollegen fand die Verbreitung auch Wege über Intranet, Telefonate und E-Mails. Das Spiel wurde zum Thema im Unternehmen. Es bekam einen ruckartig ansteigenden Zulauf, als der erste Beitrag im Firmenblog dazu erschien. Weitere, bisher unbeteiligte Mitarbeiter beteiligten sich. Bis zum Ende des zweiten Levels wurden mehr als 3.000 Quizfragen beantwortet. Insgesamt wurden 13.150 Quizfragen im Verlauf des gesamten Zeitraums beantwortet, davon 6.375 korrekt.

Verbesserungsansätze

Es ist nicht vollständig gelungen, die sehr große Zielgruppe mit den für sie passenden Inhalten zu versorgen. Bei einer Wiederholung sollte das Framework deshalb auf eine kleinere Zielgruppe angewendet werden. Der erste Schritt im Spiel war aus Gründen der Umsetzbarkeit an die Abteilungsleitung und nicht an jeden einzelnen Mitarbeiter adressiert. In Ausnahmefällen ist deshalb die Spieleinladung nicht über die Leitungsebene bis in die Abteilung vorgedrungen. Diese Erkenntnis spiegelt sich auch in der Befragung wieder, bei der 36% angaben, dass sie von dem gesamten Spielverlauf nichts mitbekommen hätten. Bei einer Wiederholung dieses Programms, scheint es empfehlenswert diese Herangehensweise zu überarbeiten. So könnte eine noch breitere Streuung erreicht werden.

Literatur

[AG13a] Aconsite AG. *Wie Sie mit aufgeweckten Mitarbeitern Datenschutzskandale vermeiden*. Website: http://www.aconsite.de/CMS/Security-Awareness.html, Abruf: 5.12.2013, 2013.

[aG13b] ausecus GmbH. *Schulungen und Workshops*. Webseite: http://www.ausecus.com/de/industrial-it-security/awareness-workshops, Abruf: 5.12.2013, 2013.

[Ble13a] Blendtec. *Video: BlendTec CEO Says Sales up 700% Since Launching: Will it Blend*. Website: http://www.youtube.com/watch?v=u6t92m1gwTY, Abruf: 5.12.2013, 2013.

[Ble13b] Blendtec. *Video: Will It Blend? – iPad*. Website: http://www.youtube.com/watch?v=lAl28d6tbko, Abruf: 5.12.2013, 2013.

[cA13] Hvs consulting AG. *Security Awareness Kampagnen*. Website: http://www.hvs-consulting.de/security-awareness-kampagnen.aspx, Abruf: 5.12.2013, 2013.

[Cha13] Bill Chamberlin. *Gamification: A 2013 HorizonWatching Trend Report. HorizonWatching and IBM*. Website: http://de.slideshare.net/HorizonWatching/gamification-a-horizon-watching-trend-report-05feb2013, Abruf: 5.12.2013, 2013.

[DGHA12] European Commission Directorate-General Home Affairs. *Cyber Security Report*. Website: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf, Abruf: 5.12.2013, 2012.

[ED13] Andreas Exter und Matthias Drodt. *CSI:DB – Die IT Security-Awareness-Kampagne der Deutschen Bahn*. Datenschutz und Datensicherheit 5.2013, 2013.

[EKR08] Martin Eisend und Franziska Küster-Rohde. Soziale Netzwerke im Internet — Marketingkommunikation für morgen. *Marketing Review St. Gallen*, 25(5):12–15, 2008.

[elT10] enspire learning Texas. *Whitepaper This Is Not A Game: Using Alternate Reality Games in Corporate Training*. Website: http://www.enspire.com/wp-content/uploads/2010/09/White-Paper-Using-Alternate-Reality-Games-in-Corporate-Training.pdf, Abruf: 5.12.2013, 2010.

[Fon12] John Fontana. *Employees would sell work password for 5 pound*. Webseite: http://www.telegraph.co.uk/technology/internet/9189236/Employees-would-sell-work-password-for-5.html, Abruf: 5.12.2013, 2012.

[fSidI03] Bundesamt für Sicherheit in der Informationstechnik. *Durchführungskonzept für Penetrationstests*. Website: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest_pdf.pdf, Abruf: 13.02.2014, 2003.

[Hal98] Gregor Halff. Ergebnis aus der Strukturierung der Involvement-Forschung: das 'Elaboration Likelihood Model' ('ELM'). In *Die Malaise der Medienwirkungsforschung: Transklassische Wirkungen und klassische Forschung*, Jgg. 28 of *Studien zur Kommunikationswissenschaft*, Seiten 175–195. VS Verlag für Sozialwissenschaften, 1998.

[HP09] Michael Helisch und Dietmar Pokoyski. *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Seite 10. kes vieweg und teubner, 2009.

[Inc13] McAfee Inc. *Security Awareness Program Development and Training*. Webseite: http://www.mcafee.com/de/services/strategic-consulting/program-development/security-awareness-program-development-and-training.aspx, Abruf: 5.12.2013, 2013.

[KS13] Robert Kaltenböck und Sabine Schuster. *Awareness für Informationssicherheit und Datenschutz in der Sparkassen-Finanzgruppe. Mit Bildsprache Mitarbeiter sensibilisieren.* Datenschutz und Datensicherheit 5.2013, 2013.

[Lan09] Sascha Langner. *Viral Marketing. Wie Sie Mundpropaganda gezielt auslösen und Gewinn bringend nutzen. 3. erweiterte Auflage*. Wiesbaden: Gabler, GWV Fachverlage GmbH, 2009.

[Mat09] Jochen Matzer. *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*. kes vieweg und teubner, 2009.

[MN90] Christian Michel und Felix Novak. *Kleines psychologisches Wörterbuch. Erweiterte und aktualisierte Neuausgabe. ISBN 3-451-08690-5*. Herder, Freiburg (Breisgau), 1990.

[mOTG13] mybreev Online Trainings GmbH. *awareness training ändert die Verhaltensmuster der Mitarbeiter*. Website: http://www.mybreev.com/de/news/awareness-training-andert-die-verhaltensmuster-der-mitarbeiter.html, Abruf:5.12.2013, 2013.

[Pet86] Cacioppo Petty. *The Elaboration Likelihood Model Of Persuasion. In: Advances in experimental social psychology*, Seiten 123–205. New York: Academic Press, 1986.

[Por12] Gartner Portals. *Gartner Predicts Over 70 Percent of Global 2000 Organisations Will Have at Least One Gamified Application by 2014. Content and Collaboration Summit, March 12-14, 2012 in Orlando, Florida*. Website: http://www.gartner.com/newsroom/id/1844115, Abruf: 5.12.2013, 2012.

[PTZ13] Polyxeni (Jenny) Palla, Rodoula H. Tsiotsou und Yorgos C. Zotos. Is Website Interactivity Always Beneficial? An Elaboration Likelihood Model Approach. In Sara Rosengren, Micael Dahlén und Shintaro Okazaki, Hrsg., *Advances in Advertising Research (Vol. IV)*, EAA Series, Seiten 131–145. Springer Fachmedien Wiesbaden, 2013.

[Ros12] Peter Rossbach. *Der Mitarbeiter als Komponente der Informationssicherheit*. Frankfurt School of Finance u. Management, 2012.

[Rup13] Benjamin Rupp. *In Frankfurter Unternehmen sorgt AirITSystems für mehr Sicherheit*. Webseite: http://www.airitsystems.de/standorte/frankfurt/security-awareness-frankfurt/, Abruf: 5.12.2013, 2013.

[Sch13] Klaus Schimmer. *Ein Poster ist zu wenig! Das Trainings- und Awareness Framework der SAP*. Datenschutz und Datensicherheit 5.2013, 2013.

[SWA05] Dorothy Stanley, Jesse Walker und Bernard Aboba. *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. RFC 4017 (Informational), http://www.ietf.org/rfc/rfc4017.txt, 2005.

[ZAO13] Kaspersky Lab ZAO. *The evolution of Phishing attacks: 2011-2013*. Website: http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf, Abruf: 5.12.2013, 2013.