OLÉ

Der Security-Newsletter
hrsg. von known_sense

12 Mai 2010

Awareness + Unternehmenskultur + Elektronische Kampfkunst

PODCAST

- **Weltpremiere:**
  „Cybarry & Samantha Safe" – bei einem internationalen Spezial-Chemiekalienhersteller wirbt ein Security Awareness Podcast in 6 Sprachen für mehr Sicherheit

- **Interview mit Manfred Schreck (Novartis):**
  „Sinnvolle Entscheidungen treffen"

- **Innovative Awareness Tools:**
  – „Quer durch die Sicherheit" in Kürze auch online.
  – Neue Moderationskarten „Talking Security" machen CISOs fit für Kommunikation

„Cybarry & Samantha Safe"

Bei einem internationalen Spezial-Chemiekalienhersteller wirbt ein Security Awareness Podcast in 6 Sprachen für mehr Sicherheit

Dietmar Pokoyski

Au, au, au, non sono mica un tamburo. Smettila di avventarti su di me... „Hör auf, auf mich einzudreschen ... War das jetzt richtig so? Oder hast du da was mit der Trommel vergessen?" Samir Saleh spricht fließend Deutsch, Französisch und Englisch und ein bisschen Spanisch. Niederländisch? Das nimmt man halt so mit – für einen deutschen Muttersprachler in der Regel kein Problem. Aber Italienisch? Fehlanzeige! Hatte er nie gelernt. Jetzt sucht er nach den richtigen Anschlüssen in einer Sprache, die er nicht spricht, die er kaum versteht. Samir ist Toningenieur und wir befinden uns im Studio der Horchposten GmbH im Hinterhof des bekannten Hörbuchladens an Rande des Belgischen Viertels in der Kölner Innenstadt.

Diejenigen, an die sich Samirs Frage richtet, heißen Luciana Caglioti und Christiano Cruciani und sind zwei von insgesamt zwölf Sprechern, die in die Rollen von „Cybarry & Samantha Safe" schlüpfen, des weltweit vermutlich ersten internationalen Security Awareness Podcasts. „Ja, war völlig in Ordnung," bestätigen Luciana und Christiano unisono. „Ok, weiter," sagt Samir. Und: „Aufnahme!"

Diese kleine Unsicherheit zu Beginn der ersten Folge bleibt eine Ausnahme. Denn die weiteren italienischen Aufnahmen – immerhin insgesamt vier Stunden – klappen wie am Schnürchen, auch, wenn Samir am Ende des Tages immer noch kein Italienisch kann. Italienisch ist die letzte von insgesamt sechs Sprachen, in denen im Horchposten-Studio ein Trailer und acht Folgen unseres Security-Podcasts aufgenommen werden. Die anderen Sprachen – Deutsch, Englisch, Französisch, Spanisch und Niederländisch – sind schon durch. Daher kennt Samir inzwischen nicht nur die Geschichten von Cybarry und seiner Kollegin Samantha Safe, sondern auch die Inhalte der meisten Dialoge und weiß, wie die ungefähr klingen müssen – auch in einer Fremdsprache. Er setzt seine Marken für die Postproduktion zunächst nach Gehör. Das Feintuning kommt später, dann, wenn er sich in seiner Muttersprache Deutsch sowie auf Basis des Skripts vergewissert hat, dass kein Dialog, noch nicht einmal eine kleine Interjektion, fehlt.

Auch ich kann Luciana und Christiano in ihren Dialogen folgen, obwohl Italienisch auch nicht zu meinem Fremdsprachen-Repertoir gehört. Als Autor der Kurz-Hörspiele im Auftrag eines internationalen Spezialchemiekalienherstellers habe ich gemeinsam mit André Helfers von Horchposten, die ansonsten u.a. die Hörbücher aus der populären Reihe „Das schwarze Auge" produzieren, die Regie übernommen. Für meine Agentur known_sense ist es die

Unsere Sprecher

Eva Maria Artega (ES)

Luciana Caglioti (I)

Christiano Cruciani (I)

Jef van Even (NL)

Jean Faure (F)

Deborah Friedman (EN)

dritte Corporate Audiobook-Produktion in knapp zwei Jahren – und die aufwändigste, nicht nur aufgrund der Übersetzungen in nahezu jede Unternehmenssprache des Auftraggebers, sondern auch aufgrund der Länge. Jede Folge dauert – mit Ausnahme des Trailers – sieben bis neun Minuten; macht zusammen eine fast volle CD mit über 60 Minuten Spielzeit – in JEDER Sprache!

Bereits 2008 hatte known_sense für das Chemieunternehmen eine internationale Security Awareness-Kampagne ausgerollt. Absender von Medien wie Plakaten, Comicpostkarten, Security-Quizzes und mehr ist als Stellvertreter des Security Managements die Leitfigur Cybarry, ein Fass als Brand mit Armen, Beinen und einem in der Regel freundlichen Gesicht. „Au, au, au. Ich bin doch keine Trommel", brüllt Cybarry zu Beginn der ersten Folge, als man ihn für ein verloren geglaubtes Fass hält, das einst Chemikalien des Unternehmens von a nach b transportiert hat. Um dann aber im weiteren Verlauf davon zu berichten, dass in seinem „langen" Leben bereits VIPs wie Diogenes oder Huck Finn in ihm gewohnt hätten und er das einzige überlebende Fass der Exxon-Valdez-Havarie sei.

Als „Maskottchen" der Security Awareness-Kampagne ist Cybarry natürlich auch ein selbst ernannter Streiter für die Sicherheit und persönlicher Security-Berater von Samantha Safe, die sich seit 15 Jahren im Firmen-Office mit ihr sinnvoll wie unsinnig erscheinenden Sicherheitsmaßnahmen herumschlägt und an einer von Dr. Tanski diagnostizierten, tückischen Passwort-Allergie leidet

Vom Jingle bis zur Quizfrage

Der Aufbau jedes Podcasts folgt einer stets einheitlichen Struktur. Zuerst ein eingängiger, gute Laune verbreitender Jingle von Harald „Sack" Ziegler, den man spätestens nach der zweiten Folge mitpfeifen muss. Ziegler, der als Komponist bereits ARD-Hörspiele und auch die known_sense-Produktion „Wir in Köln" für ein großes Medienunternehmen vertont hatte, hat die komplette Musik, neben dem Jingle diverse Moods, und darüber hinaus alle benötigten Geräusche, u.a. Raddampfer, Straßen-Athmo, Klingeltöne, etc., mit seinem Leitinstrument, dem Horn, sowie diversen Percussions, Plastik- und Blechspielzeugen u.a. Instant-Materialien, die z.T. im Studio verfügbar waren, solo in einem circa 8stündigem Aufnahmeprozess – Layer für Layer – eingespielt.

Nach dem Jingle erscheint Cybarry in Samanthas Büro. Ein alltäglicher Anlass wie z.B. das Absenden einer E-Mail oder – in Pausen – die Vorbereitungen auf eine Wichtelparty verwickelt die beiden in ein Streitgespräch, in dem es am Ende stets um ein Securitythema geht. Aufgelöst wird der sich zuspitzende Dialog zwischen dem Fass und der Angestellten durch einen Anruf von extern, der in der Regel internationale Stars wie Steven Spielberg, Muhammad Ali, Tom Cruise, Madonna oder Michelle Obama (fiktiv) auf die (Audio-)Bühne hievt. Diese Telefondialoge zwischen Cybarry und den VIPs bergen stets auch die Lösung für das jeweilige Security-Problem in sich. Z.B. behauptet Cybarry, dass Madonna ihn für Studioaufnahmen im Kontext eines Backmasking-Tracks (Anm.: ein Song mit rückwärts abgespieltem Text) verpflichten wolle (s. Kasten auf S. 5). Anhand dieser Steilvorlage erklärt Cybarry sodann Sam, wie z.B. Verschlüsselung funktioniert und wie man diese zugunsten der Informationssicherheit einsetzen sollte. Neben Verschlüsselung werden in anderen Folgen auch weitere Top-Themen der Security thematisiert und einer möglicht breiten Mitarbeiter-Zielgruppe erklärt, z.B. Passwort, Social Engineering, Informationsträger, Clean Desk oder Social Networks.

Jeder Folge schließt mit einer Quizfrage aus dem Kampagnen-Gewinnspiel, z.B. „Ein Passwort ist dann stark, wenn es die folgenden Elemente enthält? a) Anzahl an Kaffeetassen, die ich pro Tag trinke, in Zahlen? b) ... die Etage, in der ich arbeite, als Ziffer? c) ... Anfangsbuchstaben der Lieblingsspielzeuge meiner Nichten und Neffen? Oder d) .... mindestens 8 Zeichen, Groß- und Kleinbuchstaben und natürlich Sonderzeichen?"

Durch die Verknüpfung mit weiteren Medien wie dem o.g. Gewinnspiel, Postern

Unsere Sprecher(innen)

Tanja Haller (D)

Michael Holdinghausen (D)

Sara Liu (NL)

Carlos Garcia Piedra (ES)

Mark Rossman (EN)

Aurélie Thepaut (F)

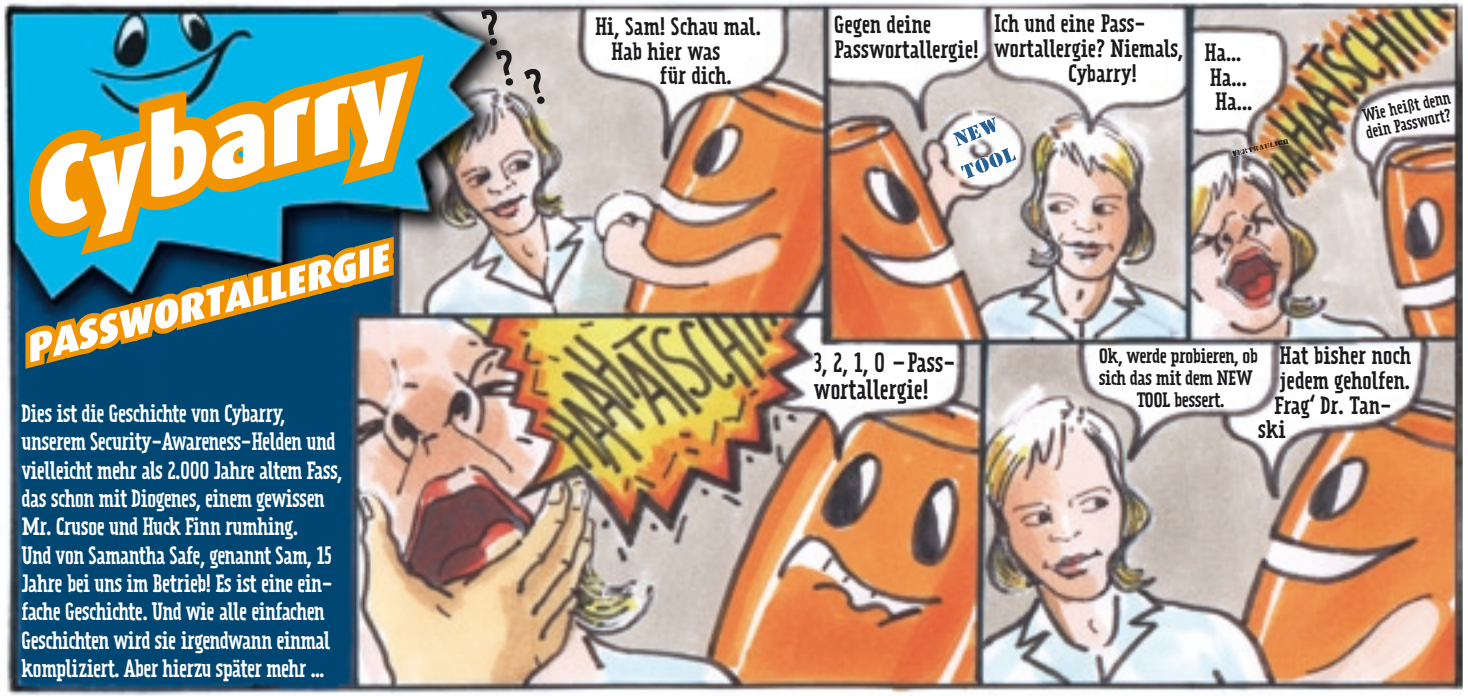
oder Comic-Postkarten, mit deren Hilfe die Mitarbeiter sich bereits seit Beginn der Kampagne ein Bild von Cybarry und Samantha machen konnten, wird der integrierte Ansatz der verschiedenen Maßnahmen und die Verknüpfung der zahlreichen beteiligten Kanäle gewährleistet, die im Zusammenwirken weltweit an circa 60 Standorten für mehr Sicherheit im Unternehmen werben.

Populäre Pop-Chiffren

„Natürlich wollen wir erreichen, dass die Kollegen die Regelwerke kennen und Tools nutzen, die den Umgang mit Security leichter und für alle sicherer gestalten", sagt Thomas Dallmann, der Information Security Manager des Auftraggebers. Und: „Der Medienmix, insbesondere das originelle Storytelling, bei dem originär eher langweilige Sicherheitsthemen mit global populären Pop-Chiffren gemixt und auf diese Weise spannend aufbereitet werden, hilft uns, den Umgang mit Security zu entkrampfen und den Mitarbeitern zu demonstrieren: ‚Da, schaut her, Informationssicherheit kann durchaus ein spannendes Thema sein, zu dem es viele Geschichten zu erzählen gibt.' Und wenn das Interesse einmal geweckt ist, kennen die Mitarbeiter hoffentlich auch die Quellen, die sie im Zweifelsfall zur Ausgestaltung ihres Secrity-Know-hows heranziehen sollen – etwa unser Intranet oder das User-Handbuch zur Sicherheit."

Storytelling als methodisches Vorgehen

Wer denkt sich aber all' diese Geschichten aus? Die Antwort ist gar nicht so schwer, sofern das Vorgehen methodisch unterfüttert ist und einer klar umrissenen Strategie folgt. Die narrativen Grundlagen für sämtliche Kampagneninhalte von der Ausgestaltung der Leitfigur bis hin zu den Storyboards für die Comics wurden bereits in



Auszug aus Folge 4: „Hung up"

C: (singt) YLWOLS OS YB SEOG EMIT

S: Huh, grusel .... das hört sich aber gespenstig an ...

C: Was singe ich denn da? (Singt nochmal von vorn)

S: ... (Pause, Sam überlegt, dann singt sie ebenfalls oder summt die Melodie, Cybarry schwenkt summend oder singend ein) Every little thing that you say or do, I'm hung up, I'm hung up on you, Waiting for your call, Baby night and day, I'm fed up, I'm tired of waiting on you ...

S: Hey, das ist "Hung up" von Madonna, rückwärts gesungen cool ..., Cybarry, ...so geht also Verschlüsselung?

C: Ja sicher. Eine klar lesbarer Information mit Hilfe eines Verschlüsselungsverfahrens in eine Art Geheimtext umgewandelt. Das Verfahren hier war „rückwärts". Nur der, der weiß, dass ich rückwärts gesungen habe, kann das Lied auch erraten.

S: Das ist ja genial ... aber ... mmmmh ...IKSNAT ... äh ...

C: ... Was meinst du ...?

S: IKSNAT ... Also TANSKI! Ich habe versucht, Dr. Tanskis Namen rückwärts auszusprechen. Und rückwärts schreiben ... hmm ... das wird aber ganz schön lange dauern, rückwärts geschrieben schaff' ich bestimmt nur eine halbe Seite am Tag ...ha ... ha ... ha (Niesanfall)

C: Gesundheit. Ah, quatsch ... Bewusstsein!

S: Ha .... Cybarry ...!

C: Unsinn! Bei den meisten Verfahren brauchst du so gut wie gar nichts unternehmen, weil das eh eine Software regelt. Bei unserer Festplatten-Verschlüsselung ebenfalls ...

S: Software ... Pooh, da bin ich ja beruhigt.

C: Cybarry hier. Oh, hallo Frau Ciccone ...Ah, schön. ... Ja ich freu mich. ... Nächste Woche schon. ... Ok .... Wo? ...In New York ... Alles klar ... Ich bin dabei ...

S: ... Ciccone ... ist das ne Kundin ...? Kenne ich gar nicht.

C: Kundin? Wenn du wüsstest ...

S: Hmmm?

C: Tja, Künstlernamen haben ja auch was mit Kryptographie zu tun ... Keine Idee ...? (stolz) Das war Madonna ...

S: Madonna? Die Sängerin ...?

C: Ja, wer denn sonst. Ich habe mich bei ihr beworben. Sie will so ein Backmasking-Track produzieren mir versteckten Rückwärtsbotschaften – die soll ich dann singen.

S: Echt wahr, Cybarry? Erst Ali, dann Madonna! Vielleicht wirst du ja ein Star? Trotz kynischer Bedürfnislosigkeit ...

C: Kann gut sein ...

S: Aber wenn du dich um Schallplatten kümmert, wer kümmert sich dann um unsere Festplatten, vor allem um diese Laptop Verschlüsselung?

Erzähler: Tja, das ist wieder eine dieser Fragen ...

der Analysephase bei der Vorbereitung der Gesamtmaßnahme gelegt. Bereits 2008 war es mithilfe tiefenpsychologisch moderierter Workshops gelungen, die Sicherheitskultur des Chemieunternehmens aufgrund von vorhandener CI, Branchenwirklichkeit, tatsächlicher Sicherheitsvorfälle und Positionierung der Security-Protagonisten zu identifizieren, zu beschreiben und im Rahmen eines sich verdichtenden Storytelling-Prozesses aus der sachlichen Dokumentation heraus in spannende Geschichten zu übersetzen.

Sicherheit gut verkaufen

Thomas Dallmann: „Im Laufe der zweiten Kampagnenphase im Herbst 2009 erschien uns allerdings das Medium Comic-Postkarte, das wir bis dato hinsichtlich des Storytellings genutzt hatten, zu begrenzt, um die z.T. komplexe Geschichte unserer Corporate Security adäquat erzählen zu können. Aufgrund meines persönlichen Interesses an Audio-Podcasts haben wir uns dann in Abwägung Hörspiel versus Videos relativ bald für die Audio-Umsetzung entschieden. So eine Podcast-Folge kann ich mir auch schon mal auf eine CD brennen und z.B. beim Autofahren hören. Das Medium erfordert auch eine höhere Konzentration als z.B. Videos, die oft wie Schulfernsehen nur durchrauschen. Daher erschienen uns gerade Hörspiele zur Umsetzung unserer Strategie und auch hinsichtlich des Transports unserer Inhalte sehr geeignet."

Im Intranet wird nun seit April 2010 bis zum Jahresende jeden Monat eine neue Folge bereit gestellt. Multiplikatoren wie z.B. Securitymanager oder IT-Verantwortliche haben bereits vorab sämtliche Folgen als CD-Edition erhalten, denn dir Mitarbeiter brauchen ja Meinungsbildner, die ihnen die Vorzüge eines Security-Podacasts verkaufen.

„Security Manager," sagt Thomas Dallmann, „sind auch nichts anderes als ‚Verkäufer' – eben von Sicherheit." Und: „Im Rahmen unseres ‚Vertriebs' ist mir jedes gute Marketinginstrument recht, um mein Anliegen an die Frau bzw. den Mann zu bringen. Unsere Podacasts werden sicher ein große Rolle dabei spielen, das Thema innerhalb des Unternehmens besser, weil lebendiger zu vermarkten." ■

Weitere Informationen und Hörproben: www.corporate-audiobook.com

„Sinnvolle Entscheidungen treffen"

„Wissensvermittlung ist wichtig, sie allein reicht uns aber nicht". Diesem Statement folgend hat sich der Fokus der Security Awareness-Aktivitäten der Novartis International AG im Laufe der Zeit verändert. Manfred Schreck, seit 2002 Head of Group Information Security, erklärt, wie sich dieser Entwicklungsprozess konkret gestaltete.

Interview: Michael Helisch

Welche Rolle spielt Security Awareness in Ihrem Aufgabenbereich im Unternehmen?

Security Awareness ist neben dem Baustein Training ein essentieller Bestandteil unserer Information Security-Strategie. In dieser Strategie haben wir verschiedene Risikothemen definiert wie z.B. Web 2.0 oder den Bereich der »consumer technology« d.h. den stationären und vor allem mobilen Werkzeugen, die von den Kolleginnen und Kollegen in ihrer täglichen Arbeit verwendet werden. Aufgabe von Awareness ist es, diese Risikothemen zu adressieren und die Umsetzung dieser Strategie zu unterstützen. Um bei dem Beispiel der »consumer technology« zu bleiben: Gerade bei neuen Technologien ist man allzu oft nicht in der Lage, sämtliche, mit der Nutzung dieser Technologien verbundenen Risiken sofort zu antizipieren. Dementsprechend existieren oftmals auch keine geeigneten Sicherheitsmassnahmen (Tools, Prozesse, Richtlinien). Aus Sicht der Sicherheit entsteht somit eine Lücke, die es zu schließen gilt. Wie tun wir das? Indem wir unsere Mitarbeiter zur »first line of defence« machen. Mittels Awareness und Training werden die Mitarbeiter zu einem wirksamen »Instrument«, um solche Sicherheitslücken zu schließen. Wir versetzen sie in die Lage, risikoadäquat zu handeln und »ihre« Informationen situationsgerecht zu schützen. Da wir in diesen »neuen, unbekannten« Bereichen nicht auf bestehende Richtlinien zurückgreifen können, sind wir bewusst abgekommen von der strikten Fokussierung auf Compliance-Bestrebungen (»Du darfst / Du darfst nicht«) und haben unseren Awareness-Ansatz stärker auf das Risikobewusstsein des Mitarbeiters (»Du kannst und entscheidest, was du tust bzw. nicht tust«) ausgerichtet. Auch der in unserer Strategie adressierte Risikobereich der wachsenden Globalisierung unseres Business beeinflusst unseren Ansatz zum Thema Awareness. Ganz konkret bedeutet das: Als Verantwortlicher einer Group Information Security-Abteilung muss ich generelle kulturelle Unterschiede der einzelnen Länder beachten, genauso wie ich die Unterschiede der einzelnen Geschäftsbereiche beachten muss. Dies erfordert eine Flexibilisierung der Art und Weise, wie Awareness in den einzelnen Novartis Geschäftsbereichen und zugehörigen Unternehmen umgesetzt wird. Training hingegen fokussiert stärker auf die Vermittlung und »Übersetzung« der Security-Vorgaben auf die security-relevanten Geschäftsprozesse. Was sollte ich als Mitarbeiter der IT bei der Entwicklung von Applikationen aus Sicherheitssicht beachten? Was bedeutet Sicherheit in meiner täglichen Arbeit als Mitarbeiter im Bereich Personal? Um Fragen wie diese geht es hier beispielsweise. Unser Training in diesem Bereich ist also sehr viel stärker auf spezielle Zielgruppen wie IT, Personalabteilungen etc. und spezielle Richtlinien für diese Bereiche ausgerichtet. Unsere Information Security Manager und alle Mitarbeiter, die mit sensitiven Informationen umgehen, müssen über entsprechendes Know-How

verfügen, um dies dann in den relevanten (Business-)Prozessen adäquat anwenden zu können.

Wenn Sie Security Awareness definieren müssen – wie würde Ihre Definition lauten?

Ich mache es daran fest, was ich mit Awareness erreichen möchte. Hier würde ich als Ziel formulieren: Der Mitarbeiter macht die Dinge intuitiv richtig d.h. geht mit Informationen sicher um. Um in der Information Security wirklich nachhaltig voran zu kommen, muss ich den Mitarbeiter in die Lage versetzen, sinnvolle Entscheidungen zu treffen, bei denen er selbst Risiko-, Business- und sonstige relevante Aspekte abwägt und dann entsprechend handelt. Für das Unternehmen wird der Mitarbeiter so zum Risk Manager derjenigen Informationen, mit denen er tagtäglich umgeht. Der andere Teil meiner persönlichen Definition von Security Awareness beschreibt den Weg dorthin und die Mittel, die ich dazu brauche. Er beschreibt somit den Prozess der Awareness. Awareness benötigt allerdings nicht zwangsläufig immer Richtlinien, da es schlichtweg unmöglich ist, alle Risiken über Regeln erfassen zu können bzw. zu wollen.

Was war der Auslöser bzw. die Motivation für die Umsetzung von Security Awareness-Maßnahmen und welche konkreten Ziele sollten erreicht werden?

Da gibt es verschiedene Aspekte, die im Zeitraum der letzten acht bis zehn Jahre relevant waren. Unsere grundlegende Motivation bestand aber darin, die Mitarbeiter mit dem Thema Information Security vertraut zu machen. In der ersten Phase, also ab 2002 ging es zunächst im Rahmen von web-based trainings darum, den Novartis-Mitarbeitern ein relativ umfangreiches Sicherheits-Regelwerk einfach und verständlich zu vermitteln. Diese reine Wissensvermittlung hat uns aber nicht genügt. So lag der Fokus der zweiten Phase auf der Frage, wie wir uns weiter verbessern können. Unter dem Motto »small steps for improvement « wurde ein Programm ins Leben gerufen, das auf kleine Teams in den Geschäftsbereichen ausgerichtet war. Im Rahmen einer einstündigen Team-Session wurden typische, sicherheitsrelevante Problembereiche (z.B. »Tailgating« oder Verwendung »schwacher Passwörter«) dargestellt und deren Folgen geschildert. Das Team sollte nun selbst die Frage beantworten: Wie sieht es in unserem Bereich aus? Was können, was werden wir im Hinblick auf die uns betreffenden Probleme tun? Innerhalb der nächsten Wochen sollte dann im Rahmen einer gemeinsamen Teamvereinbarung ein entsprechender Aktionsplan erarbeitet werden. Die Problembearbeitung und damit die Verhaltensänderung erfolgte somit aus dem Team heraus. Wichtig dabei war, dass das Team selbst die Verantwortung für die Umsetzung der von ihm festgelegten Maßnahmen übernommen hat. In der dritten Phase geht es nun darum, die Mitarbeiter zu der bereits erwähnten »first line of defense« zu machen. Anhand ausgewählter Situationen wie z.B: der Benutzung von mobile Devices wird aufgezeigt, welche Risiken existieren und wie sicherheitskonformes Verhalten aussehen kann. Den Mitarbeitern werden damit konkrete Entscheidungshilfen für ihren beruflichen Alltag mit an die Hand gegeben. Den Inhalt der vierten Phase, die mehr oder weniger parallel zu »first line of defense«» läuft, erarbeiten wir zielgruppenspezifische Trainingseinheiten für Prozess-Experten wie z.B. die Information Security Officer, Mitarbeiter im Bereich Personal oder Anwendungsentwickler. Es geht hier also um ein proaktives Adressieren von Mitarbeitern in Rollen mit besonderer Sicherheitsrelevanz. Was wir laufend tun ist, aktuelle Sicherheitsvorfälle aufzugreifen und das richtige Verhalten in den entsprechenden Medien wie z.B. in unserem Information Security Webportal zu erläutern. Die Klickraten zeigen, dass dieses Angebot von den Kollegen dankbar angenommen wird. Als Group Information Security-Abteilung ist es unser Ziel, dass das umfangreiche Awareness-Material zukünftig verstärkt von allen Information Security Officern in der globalen Organisation genutzt wird.

Welchen Ansatz zur Vorgehensweise haben Sie gewählt und warum?

Die Initiative für die Awareness-Maßnahmen kam aus der Group Information Security, somit von uns selbst. Wir haben es als nötig erachtet, hier entsprechende Schritte einzuleiten und haben unser Anliegen an der richtigen Stelle platziert. Die Organisationsstruktur des Novartis-Konzerns mit seinen verschiedenen Geschäftsbereichen

und Unternehmen bringt es mit sich, dass die Umsetzung der Information Security-Strategien und Vorgaben dezentral durch die Information Security Officer erfolgt. Dabei passen die Information Security Officer diese Vorgaben natürlich den Anforderungen vor Ort an. Dafür stellen wir im Awareness-Bereich z.B. eine Tool-Box zur Verfügung aus dem sich der Information Security Officer vor Ort bedienen kann.

Wie sind Sie an die Planung der Awareness-Kampagne herangegangen?

Das Programm mit seinen vier Phasen haben wir mehr oder minder »step by step«, aus unserer eigenen Erkenntnis heraus entwickelt. Dabei haben wir die erforderlichen Aktivitäten weitestgehend selbst definiert und umgesetzt. Die Zusammenarbeit mit unserer eigenen Kommunikationsabteilung erfolgt erst seit jüngster Zeit und da im Speziellen, wenn es um die Umsetzung von Kampagnen geht.

Was haben Sie genau gemacht?

Das »web-based training« wurde extern gemäß unserer Anforderungen entwikkelt. Branding-Aspekte bleiben dabei unberücksichtigt. Für das »small steps for improvement«-Programm wurde gezielt ein eigenes Branding entwickelt, das durch seine Farbgestaltung die gewünschte Aufmerksamkeit im Unternehmer erzielte. Dieses Programm wurde auf Basis eines »train the trainer«-Ansatzes mittels webcasts für Information Security Officer umgesetzt. Jeder Trainer vor Ort hat einen Trainingskoffer zzgl. diversen Awareness-Materialien wie Poster, Präsentationen, Leaflets etc. zur Verfügung, welche er in den Training Sessions nach Bedarf einsetzen konnte. Ursprünglich geplant war, dass die Information Security Officer die Abteilungsleiter schulen sollten, um sie in die Lage zu versetzen, die entsprechenden Team-Sessions durchzuführen. Dem konnten die Abteilungsleiter oft aber nicht nachkommen. So wurden die Team-Sessions oft durch die Information Security Officer umgesetzt. Der gewünschte Effekt, nämlich die eigenständige Entwicklung der Maßnahmen aus dem Team heraus, wurde damit nur eingeschränkt erzielt. Für die »first line of defence«-Kampagne wird das bereits vorhandene Branding genutzt. Mittels Filmen und begleitender Maßnahmen wie Poster, Mailings, »Lunch Sessions«, werden aktuelle Beispiele wie Social Engineering, Mobile Business oder E-Mail-Nutzung anschaulich thematisiert. Ein stabiles Moment über alle Phasen hinweg ist unser Webauftritt, der vor allem die Funktion eines Werkzeugkastens für die Information Security Officer hat, aber auch für die direkte Information unserer Mitarbeiter verwendet wird.

Verraten Sie uns etwas über die Kosten Ihrer Maßnahmen und/oder über den zeitlichen/personellen Aufwand?

Die Kosten für das WBT beliefen sich auf ca. 1,00 Franken pro Mitarbeiter. Für das »small steps for improvement«-Programm wurden etwa 2,50 Franken pro Mitarbeiter ausgegeben. Die laufenden Kosten auf Group Information Security-Ebene beziffern wir auf ca. 0,35 Franken pro Mitarbeiter und Jahr. Dies beinhaltet keine Personalkosten und nicht die Kosten, die vor Ort bzw. in den einzelnen Ländern anfallen. Diese sind nur schwerlich zu beziffern. Die Verantwortung für die Planung und Koordination aller Awareness- und Trainings-Aktivitäten liegt bei Group Information Security, wofür wir in der Vergangenheit etwa 130 Projekttage pro Jahr veranschlagt haben.

Wie schätzen Sie den Erfolg Ihrer Awareness-Kampagne ein?

An der Stelle kann ich nur mit weichen Faktoren argumentieren. Wenn mich also ein Novartis-Manager fragen würde, was wir mit den Investitionen in Awareness und Training erreicht haben, so kann ich ihm keinen schlüssigen, im Sinne von nachprüfbaren Beweis für den Erfolg liefern. Das liegt allerdings in der Natur der Sache. Da wir auch keine Maßzahlen definiert haben, kann ich die Frage nach dem Erfolg nicht wirklich beantworten. Was jedoch das WBT anbelangt, so haben wir hier mittlerweile eine Abdeckung von ca. 90 % aller Mitarbeiter. Von den neuen Mitarbeitern haben ca. 70 % die entsprechenden Informationsveranstaltungen durchlaufen. Was das Thema Erfolgsmessung via Umfragen anbelangt, bin ich der Meinung, dass die Mittel sinnvoller in Konzeption und Umsetzung von Awareness-Aktivitäten investiert sind. Die Awareness-Ressourcen sind schon knapp genug – der Mehrwert bzw. die Aussagekraft von Umfragen rechtfertigt den Aufwand, den sie verursachen, aus meiner Sicht nicht. In Summe ist meine Einschät-

zung diejenige, dass wir das Bewusstsein für Information Security geschärft haben. Das zeigt mir nicht zuletzt auch die deutlich gestiegene Zahl der Anfragen, die wir erhalten, unter denen z.T. auch recht kritische sind. Man sieht also, die Kolleginnen und Kollegen setzen sich mit dem Thema auseinander.

Wer hat Sie unterstützt?

Punktuell haben wir externe Unterstützung in Anspruch genommen. So z.B. bei der Erstellung von Artikeln für Newsletter, bei der Erstellung von grafischen Arbeiten, neuerdings bei der Schulung der Information Security Officer. Der Kern der Awareness-Kampagne wurde ebenfalls extern bezogen. Meiner Ansicht nach sollte der Information Security Officer 50% seiner Zeit für Awareness aufwenden, was in der Realität allerdings oftmals anders aussieht. Die Zusammenarbeit mit dem Betriebsrat und der Personalabteilung war durchweg positiv. Ggf. auftretende Ängste oder Vorbehalte seitens des Betriebsrats, die Mitarbeiter würden durch uns in welcher Form auch immer kontrolliert, gab es bei uns nicht.

Was waren die größten Hürden bei der Realisierung? Welche Highlights gab es?

Als große Hürde erwies sich die Tatsache, dass die Organisationsstruktur der Novartis AG sehr diversifiziert ist. Novartis agiert global in einer Vielzahl von unterschiedlichen Geschäftsgebieten mit einer großen Zahl an Unternehmen. Das macht die einheitliche Umsetzung einer zentralen Kampagne wie diese sehr komplex. Als komplex erwies sich auch der Faktor der kulturellen Unterschiede. Novartis agiert in 140 Ländern und damit in ganz unterschiedlichen Kulturkreisen. Wie verpacke ich die Botschaften, damit sie in einem solch diversifizierten Umfeld auch ankommen? Ebenfalls kein leichtes Unterfangen. Flexibilität in der Umsetzung von Awareness ist daher dringend erforderlich.

Sind neue/weitere Maßnahmen geplant? Wenn ja, welche?

Wir haben in den letzten zwei Jahren sehr viel Material angesammelt. Dieses Material wird künftig verstärkt eingesetzt werden. Des weitern werden wir die inhaltliche Ausrichtung der Awareness-Kampagne verändern d.h. weg vom »Silodenken« im Sinne von: Information Security adressiert dieselben Zielgruppen ausschließlich mit seinem Anliegen, Datenschutz adressiert die Sicht des Datenschutzes, dito bei IT Security usw. hin zu einer organisationsübergreifenden und vor allem prozessbezogenen Informationsvermittlung aus einer Hand. Awareness wird zukünftig stärker aus der Sicht des Anwenders erfolgen. »Wo können wir (als Verbund von internen Organisationseinheiten, die sich um die verschiedenen Facetten des Themas Risiko kümmern) in deinem Arbeitsumfeld Hilfe leisten?« wird zum Maß der Awareness-Aktivitäten.

Was würden Sie zukünftig anders machen und welche Unterstützung, Methoden oder Tools wünschen Sie sich für zukünftige Maßnahmen?

Ich würde mehr Zeit für Konzeption und Methodik aufwenden und würde früher mit Werbe- und Schulungsfachleuten wie auch mit unseren Kollegen aus der Kommunikationsabteilung zusammenarbeiten. Einen themenspezifisches Tool-Set, dessen Inhalte an den Belangen der Mitarbeiter ausgerichtet sind, wie auch einen »Werkzeugkasten«, der denjenigen, der Awareness umsetzt, unterstützt, halte ich für sehr hilfreich.

Wollen Sie unseren Lesern noch einen Tipp auf den Weg geben?

Auch wenn das ein Allgemeinplatz ist: Awareness sollte so umgesetzt werden, dass man selbst das Gefühl hat, es bringt einen echten Mehrwert. Als Verantwortlicher im Bereich Security ist man Verkäufer einer Sache, die (zunächst) keiner haben möchte und die keiner benötigt (solange nichts passiert). Dessen sollten Sie sich bewusst sein. ■

Das Interview führte Michael Helisch am 16.12.2008 in Basel.

Auszug aus:

Helisch, Michael und Pokoyski, Dietmar (Hrsg.): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg + Teubner, 2009.

(Mit freundlicher Genehmigung des Verlags)

Abb. S. 6-9 mit freundlicher Genehmigung der Novartis International AG

Wieder lieferbar:

Helisch, Michael und Pokoyski, Dietmar (Hrsg.): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg + Teubner, 2. Auflage, 2010. 317 Seiten, 49,40 EUR. ISBN: 978-3834806680.

„Quer durch die Sicherheit" in Kürze auch online

Das Mitarbeiter-Mitmach-Riesen-Event-spiel »Quer durch die Sicherheit« wird in Kürze auch in einer Online-Version verfügbar sein.

Zur Zeit wird das Spiel redesigned und entsprechend aufbereitet. Nach Launch wird es möglich sein, die Online-Variante neben oder mit der haptischen Form zu lizenzieren – z.B. zur Nutzung im Corporate Intranet des Lizenznehmers.

Beim Branding sind neben Logo-Einbindung auch Farben und Fonts und darüber hinaus auch die Inhalte, bisher 147 Fragen zum Thema Security, individuell konfektionierbar.

Nach der EnBW setzen auch die Schweizer ISPIN AG und seit Anfang 2010 die BAKOEV, das Ausbildungsinstitut des BMI, das Spiel für Schulungen im Rahmen Ihrer Awareness-Aktivitäten ein.

http://www.known-sense.de/quer_durch_die_sicherheit_folder.pdf ■

Neue Moderationskarten „Talking Security" machen CISO & Co. fit für Kommunikation

„Welche Farbe hat Sicherheit"? „Kennst du das Passwort eines Kollegen oder eines Familienmitglieds?" „Wie sicher fühlen wir uns beim Arbeiten zu Hause?". Drei von insgesamt mehreren Dutzend Fragen zum Thema Security, die im Rahmen eines Moderationssets in einer Größenordnung von 32 bis ca. 100 Fragen in einer Kartenbox ab einer Auflage von 600 Exemplaren via aware-house lizenzierbar sind.

„Talking Security" heißt dieses neue Tool, das anlog der bekannten Reihe „Gesprächsstoff" die Security-Worker in den Unternehmen dazu anhalten soll, mit Ihren Mitarbeitern mehr und qualitativ tiefer über das Thema Sicherheit zu sprechen.

Hierbei handelt es sich nicht um ein Quiz mit standardisierten Antworten, sondern um einen systemischen Kommunikationsbeschleuniger, der sowohl im Rahmen von Team-Meetings, aber auch als „Instant-Reminder" innerhalb von Flurfunk-Kommunikation eingesetzt werden kann. http://www.known-sense.de ■

aware-house auf secAware

known_sense wird gegemeinsam mit HECOM Security Awareness Consulting ein Sponsoring der 2nd International Workfference of Security Awareness, „secAware" (29.-30.09.2010) übernehmen und dort – wie bereits im letzten Jahr – einen Workshop zum Thema Securitykultur anbieten. http://secaware.get2us.com ■

Awareness in Brandenburg

An der FH Brandenburg haben Ivona Matas, bei known_sense zuständig für die psychologische Forschung, Dietmar Pokoyski und Michael Helisch am 16. und 17. April 2010 einen Security Awareness Workshop durchgeführt. Wiederholung in Kürze! http://www.fh-brandenburg.de ■

Neuerscheinung

„Konfliktmanagement für Sicherheitsprofis" heißt das sehr zu empfehlende Erstlingswerk unserer „Wölfe-und-Geißen"-Stammkraft Sebastian Klipper. Eine ausführliche Rezension des bei Vieweg und Teubner erschienen Buchs folgt in in der nächsten Ausgabe. http://blog.psi2.de/ ■

IMPRESSUM Herausgeber: Dietmar Pokoyski (known_sense) I Kaiser-Wilhelm-Ring 30-32 I D-50672 Köln I Fon +49 221 91277778 I sense@known-sense.de I www.known-sense.de I www.aware-house.com