Ausgabe 4/2009 (40) Zweimonatsmagazin Juli/August 2009 Deutschland EUR 9,50 Österreich EUR 10,90 Luxemburg EUR 10,90 Schweiz CHF 18,60

hakin9

ABWEHRMETHODEN HARD CORE IT SECURITY MAGAZINE

BIOMETRIE-UPDATE 2009

VERFAHREN, TRENDS, CHANCEN UND RISIKEN

SECURITY AWARENESS
STEHT DER MENSCH WIRKLICH IM MITTELPUNKT?

AUTHENTIFIZIERUNG UND SESSION HANDLING

PRINT YOUR SHELL

PLUS

HTTP TUNNEL
OSSTMM 3.0

AUF DER CD

- EDPR-TESTVERSION
- DISK CLEANER 2009
- PYROBATCHFTP222
- 1-ABC.NET FILE ENCRYPTER 2.01

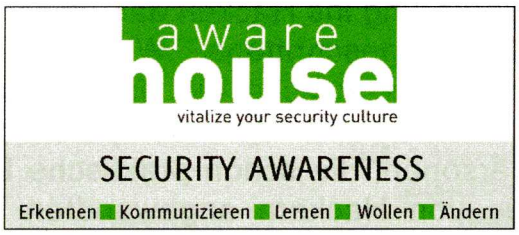
ISSN 1731-7150
05
9 771734 766326

MICHAEL HELISCH,
DIETMAR POKOYSKI

Security Awareness – steht der Mensch wirklich im Mittelpunkt?

Schwierigkeitsgrad:

Der so genannte „Faktor Mensch" ist in den letzten Jahren zum Lieblingsargument einer technisch sozialisierten Security--Branche stilisiert worden.



Die Menschen zu verstehen, sie für Security – Botschaften zu erreichen – und das ist nicht nur auf eine kognitive Art, sondern in dem Wissen um ALLE relevanten Faktoren wird gerne als DER Erfolgsfaktor der Informationssicherheit dargestellt. Die entscheidende Frage ist allerdings: Wie macht man aus „Betroffenen" in Sachen Sicherheit aktiv „Beteiligte" – und das nicht nur im Hier und Jetzt, für den Moment sondern langfristig? Welches methodische und praktische Vorgehen empfiehlt sich hier?

Was erhofft sich der Sicherheitsverantwortliche von Awareness-Kampagnen, die oft mit viel Phantasie und Kreativität umgesetzt werden? Alle Mitarbeiter (inklusive der Führungskräfte) sollen die in mehr oder weniger epischer Breite definierten Sicherheitsrichtlinien und -prozesse leben d.h. ihr eigenes Verhalten in ihrem beruflichen Alltag danach ausrichten.

Da dies per Anweisung nur bedingt funktioniert, versucht man, die Mitarbeiter mit affirmativen Gebotspostern, Schulfernsehen, öden Schulungen bzw. Pflicht-WBTs oder ins Intranet überführten Policies zu überzeugen. Scheut man selbst diesen Aufwand, erfolgt im Rahmen des allwöchentlich stattfindenden Team-Meetings eine kurze Erwähnung, dass Informationssicherheit wichtig sei und die Mitarbeiter zukünftig entsprechend handeln sollen (auch das ist leider Gottes die Realität!). Was ist damit erreicht? Nicht wirklich mehr als eine kurzfristige Aufmerksamkeit, eine auf den Moment beschränkte Einsicht, dass Informationssicherheit nicht ganz unwichtig ist. Einen wirklich nachhaltigen Effekt hat dieses (eher hilflose) Vorgehen jedoch nicht. Selbst bei aufwändigen Kampagnen sollte klar sein, dass nach der Kampagne Aufmerksamkeit und Interesse am Thema Sicherheit recht schnell abnehmen, mithin beim Mitarbeiter immer weniger „hängen bleibt", sofern nicht mit geeigneten Methoden und Maßnahmen gegengesteuert wird. Was aber kennzeichnet geeignete Methoden und Maßnahmen?

„Gehe zurück auf Los!" Ganz am Anfang steht die Frage, was sicherheitsrelevantes, menschliches Verhalten im Berufsalltag beeinflusst.

Es geht somit darum, hinter die Kulissen menschlichen Handelns zu schauen, um Sicherheitsanforderungen und tatsächliches Verhalten dauerhaft miteinander in Einklang zu bringen. Ein geeignetes methodisches Vorgehen bietet in diesem Zusammenhang beispielsweise die Gestaltpsychologie und Morphologie sowie prozessorientierte Methoden der Kommunikationsbeschleunigung. Denn Tiefenpsychologische Security-Wirkungsanalysen, systemisches CISO-Coaching, parado-

IN DIESEM ARTIKEL ERFAHREN SIE...

Was Security Awareness ist.

WAS SIE VORHER WISSEN/ KÖNNEN SOLLTEN...

Kein spezielles Vorwissen.

xe Interventionen und Prozess-Baukästen mit Modulen wie Learning Maps, Storytelling, Game Based Development (Unternehmensspiele) sind Vorgehensweisen, mit denen man hinter besagte Kulissen schaut. Sie sind in der Lage, die unbewussten, „geheimen" Faktoren der Corporate Painpoints (z.B. Mitarbeiter-Entsicherungen u.a.) aufzudecken und Kommunikationsprozesse zu optimieren. Denn wenn man schon von einer Sicherheitskultur ausgeht, möchte man auch wissen, WIE man die Besonderheiten der eigenen Kultur in Kommunikation, in Kontakte übersetzen kann, die die Mitarbeiter auch erreichen, weil sie sie be-rühren. Daher ist das Wissen um unternehmerische Wirkungseinheiten, Verfassungen, Figurationen, Haupt- und Nebenbilder, Geschichten, die im Unternehmen kursieren, und Spiele wichtig. Sie unterstützen die Unternehmen darin, das oft Gedachte, vielleicht Gesagte und manchmal Gefühlte endlich zu thematisieren. Und spielerisch lernt es sich, wie jeder weiß und (hoffentlich) am eigenen Leib erfahren hat, einfach leichter. So besteht ein Aufgabe von Awareness Kampagnen auch darin, die drei ehemals getrennten Bereiche Arbeit, Lernen und Spielen einander näher zu bringen – auch, um den „Lernertrag" der Mitarbeiter, die kognitive Basis der Awareness, zu erhöhen.

Um zu vermeiden, dass Awareness--Maßnahmen entwickelt werden, die in der Folge nicht oder nur bedingt im besagten Berufsalltag der Mitarbeiter durch selbige anwendbar sind, gehört an den Anfang jeglicher Awareness-Aktivitäten auch die Frage: „Was kennzeichnet Ihre Sicherheitskultur?" Eine differenzierte und konsequente Auseinandersetzung mit Unternehmenswerten und -kultur und den Menschen, die diese Kultur ausmachen, ermöglicht es im weiteren Verlauf der Awareness-Aktivitäten die „richtigen", d.h. die zum Unternehmen passenden Sensibilisierungsmaßnahmen zu entwickeln. Hier darf ohne weiteres etwas mehr Gehirnschmalz investiert werden, denn die Investition an dieser Stelle wird sich in der Phase der Implementierung bezahlt machen.

Awareness ist auch Kommunikation. Dabei macht in erster Linie der Empfänger und nicht der Sender die Botschaft, denn schließlich soll der Köder ja dem Fische schmecken und nicht dem Angler. Wenn schon die Werbetrommel für Sicherheit gerührt werden soll, dann aber bitteschön nicht nur oberflächlich. Aufmerksamkeit ist zwar ein wichtiges und richtiges Element im Rahmen von Awareness-Aktivitäten, die Frage ist nur, wie Aufmerksamkeit und Interesse möglichst effizient erzeugt und beibehalten werden. Mache ich mir systematisch darüber Gedanken, welches Kommunikationsmedium welche Wirkung bei welcher der Zielgruppe hat, wie die einzelnen Medien und Werkzeuge am besten zusammen wirken oder verwende ich einfach das, was der übliche Fächer der Unternehmenskommunikation hergibt?

Awareness kann und muss involvieren, heißt auch „Kontakt" – sonst passiert gar nichts! Ja, das bedeutet: Hausarbeiten erledigen und zuerst die Policy so zu transportieren, dass sie von den Mitarbeitern verstanden wird. Soll das Verstandene auch langfristig erinnert und umgesetzt werden bedarf es zweier weiterer Zutaten: Erlebnis und Emotion – sowohl über den Inhalt als auch über die Verpackung. Sensibilisierungsmaßnahmen sollten an bewusst gewählten Stellen vom unternehmenskulturellen „Mainstream" abweichen, um Aufmerksamkeit und Interesse zu wecken sowie eine aktive und nachhaltige Auseinandersetzung jedes einzelnen Mitarbeiters mit dem Thema Sicherheit zu bewirken.

Das bewusste Spiel mit unternehmenskultureller Konformität und Non-Konformität von Security Awareness-Maßnahmen ist also eine Option, sich in den Arbeitsalltag der Mitarbeiter zu drängen. Angesichts der Tatsache, dass für ein Dazwischendrängen kein „Kochrezept" existiert, ist es umso wichtiger, dass der Awareness-Verantwortliche (oder seine Berater) über die entsprechende Sensibilität verfügen, genau zu wissen, was im Hinblick auf die Zielerreichung aus Sicherheitssicht sinnvoll ist respektive der Unternehmenskultur sowie der Unternehmenskommunikation (noch) zugemutet werden kann.

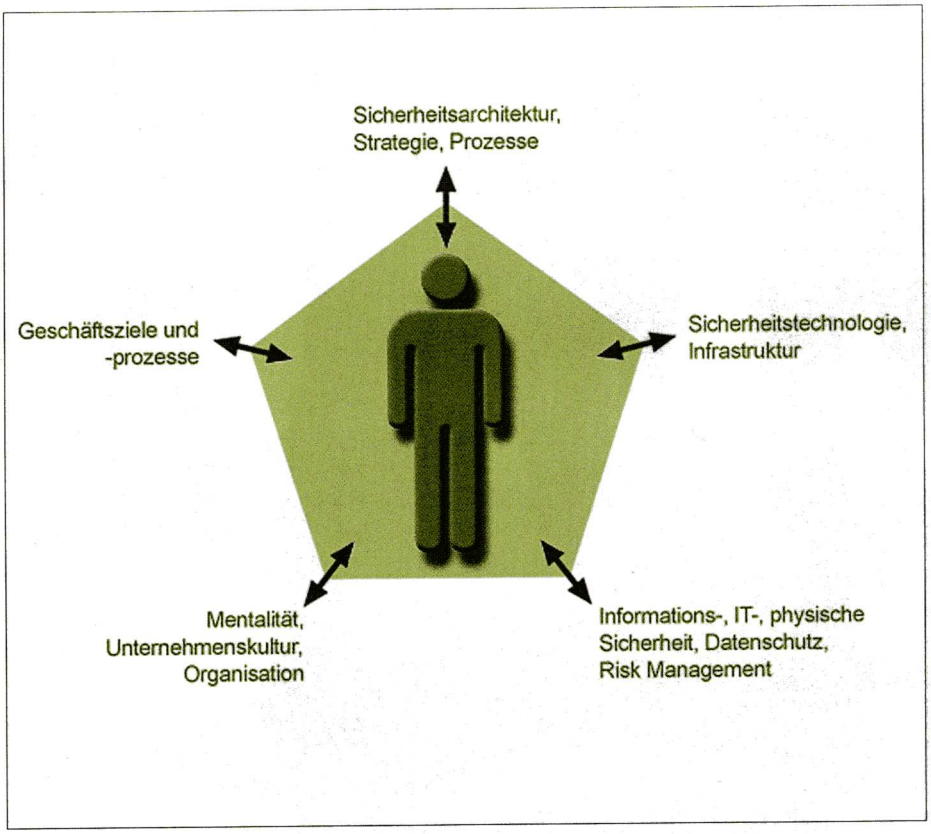
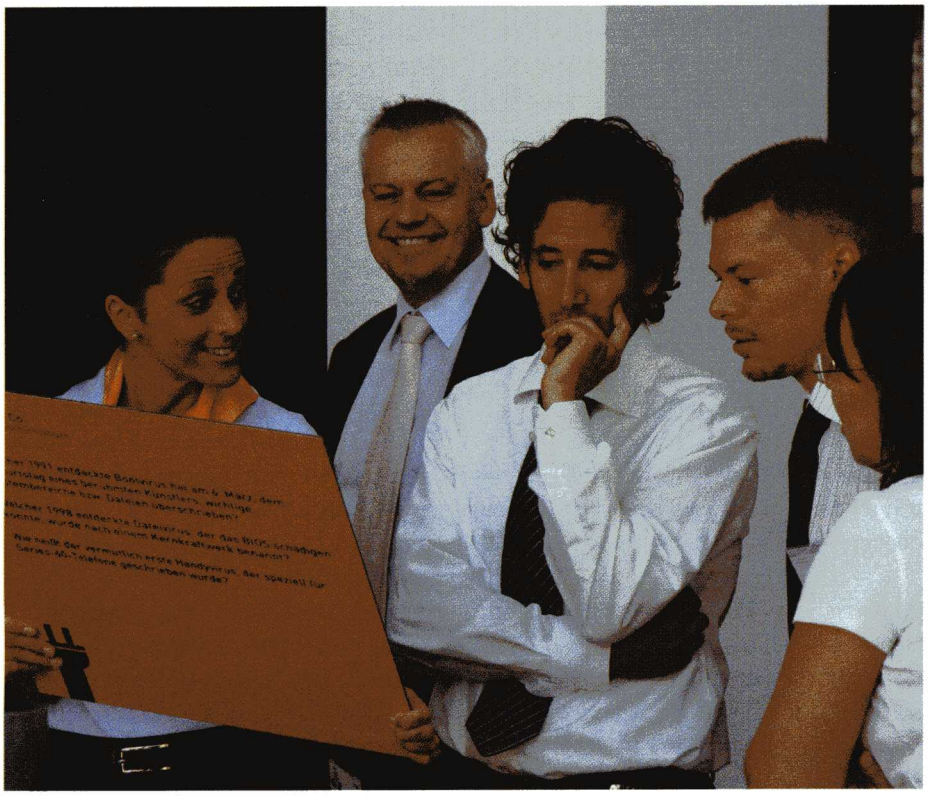


Abbildung 1. *Sicherheitskonformes Verhalten – eine mehrdimensionale und ganzheitliche Aufgabe in deren Mittelpunkt der Mensch steht.*
(Abbildung: © HECOM Security Awareness Consulting)

Fazit

Interesse für Sicherheit zu wecken, dieses Interesse in Involvement zu verwandeln und Wissen zielgruppengerecht zu vermitteln sind wichtige und richtige Aspekte von Security Awareness. Die Rahmenbedingungen zu schaffen, damit derart sensibilisierte Mitarbeiter ihr Wissen und Wollen in der täglichen Arbeit umsetzen können, ist eine weitere,

wenn nicht die größte Herausforderung erfolgreicher Awareness-Arbeit. Hierbei geht es um mehr als nur um Sicherheit. Es geht darum, hinter die Kulissen menschlichen Handelns im Unternehmen zu schauen, Unternehmensprozesse und -kultur zu hinterfragen und via Change Management in eine ganzheitliche Passung zu überführen. Dies vermag eine zeitlich begrenzte Kampagne nicht zu leisten. So wird Security Awareness zu einem stetigen und langfristigen, niemals endenden Prozess. Das der Sicherheitsverantwortliche dabei seinen originären Verantwortungsbereich verlässt und sich auf mitunter ungewohntes Terrain begibt, liegt auf der Hand. Entsprechend konsequent voran zu schreiten, erfordert Mut und Ausdauer. Dieser Mut führt letzten Endes aber zu den besseren Ergebnissen nicht nur in Bezug auf das Thema Sicherheit sondern auch für das ganze Unternehmen. Security Awareness ist damit ein Stück weit Loyalitäts- und Unternehmensentwicklung.



Michael Helisch
beschäftigt sich seit 2002 mit dem Thema Security Awareness und dabei insbesondere mit der Frage, mit welchen Methoden und Maßnahmen Security Awareness in der betrieblichen Praxis nachhaltiger umgesetzt werden kann als dies üblicherweise der Fall ist.

Dietmar Pokoyski
ist Geschäftsführer der Kommunikationsagentur known_sense aus Köln, die sich auf interne Kommunikation und Employee Branding mit Fokus auf Awareness-Maßnahmen spezialisiert hat.

Abbildung 2. *Praxisbeispiel EnBW – Energie Baden-Württemberg AG: Awareness-Spiel „Quer durch die Sicherheit" (Fotos: EnBW AG/Artis, Uli Deck)*