Michael Helisch | Dietmar Pokoyski (Hrsg.)

Security Awareness

Edition <kes>

herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im Secu-Media Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

ITIL Security Management realisieren
Von Jochen Brunnstein

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

IT-Risiko-Management mit System
Von Hans-Peter Königs

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Profikurs Sicherheit von Web-Servern
Von Volker Hockmann und Heinz-Dieter Knöll

www.viewegteubner.de

Michael Helisch | Dietmar Pokoyski (Hrsg.)

Security Awareness

Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung

Mit 244 Abbildungen

Beiträge von Marcus Beyer, Ankha Haucke,
Michael Helisch, Dietmar Pokoyski, Kathrin Prantner

Präambel von Wolfgang Reibenspies

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

Umschlagbild: © rebel / PIXELIO, www.pixelio.de
Alle weiteren Abbildungen mit freundlicher Genehmigung der jeweiligen Unternehmen
Infografiken & Layout: Carina Linnemann, Dietmar Pokoyski (known_sense)

1. Auflage 2009

Lektorat: Christel Roß | Sybille Thelen

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: STRAUSS GMBH, Mörlenbach
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0668-0

Präambel

Der Mensch ist die wichtigste Komponente der Security und damit der Schlüsselfaktor.

Damit wird der Mensch zum höchsten Gut, das Unternehmen im Kampf gegen Angriffe, die mittels Informations- und Kommunikationstechnologien geführt werden, schon heute auf der Habenseite verbuchen und damit einsetzen können. Nur durch die Menschen sind die wertschöpfenden Prozesse zu gestalten und sicher zu stellen.

Daneben ist der Mensch, glaubt man einschlägigen Studien, das größte IT- bzw. Informationsrisiko. Das Sicherheitsbewusstsein ist demnach der entscheidende Faktor zum Schutz der Unternehmenswerte und der Wertschöpfung.

Schon Kevin Mitnick schrieb: »Human Firewalls are a must!«. Frei übersetzt: »Security findet im Kopf statt – und nicht in der Technik.« Informationssicherheit ist eine Sache des Bewusstseins – und nicht der Technologie. Security ist letztendlich Loyalität.

Ergo: Awareness ist Loyalität und damit eine Frage der Unternehmenskultur. Welche Chancen hierin bestehen, aber auch, welche Störungen und mögliche Schieflagen zu berücksichtigen sind, wird in diesem Buch sehr treffend beschrieben.

Wolfgang Reibenspies

Konzernbevollmächtigter IuK-Security

IuK Security Manager

EnBW Energie Baden-Württemberg AG

Vorwort

Das vorliegende Buch handelt – vereinfacht – von der Art und Weise, wie mit dem Thema Informations- bzw. Unternehmenssicherheit mit besonderem Fokus auf den Faktor Mensch im unternehmerischen Alltag umgegangen wird. Das Buch erhebt dabei nicht den Anspruch, einen Leitfaden oder ein Lehrbuch im Sinne einer Abhandlung standardisierter Vorgehensweisen darzustellen. Standardisierung ist nach Auffassung der Autoren kein Erfolg versprechender Ansatz für Security Awareness. Vielmehr lebt die Awareness-Arbeit von ihrer Individualität. Den oder die einzig richtigen Lösungswege wird man vergeblich suchen, hingegen einen Fächer von Möglichkeiten, deren Einsatz sich je nach unternehmensindividueller Situation und Zielsetzung empfehlen. Insofern berichtet das Buch zum einem über die aus Sicht der Verfasser besonders relevanten, theoretischen und praktischen Hintergründe von Awareness. Es liefert zum anderen einen Ausschnitt »angewandter Awareness«, derer sich der Leser bedienen kann aber nicht muss. Das Buch soll also weder aufdrängen noch belehren, es soll dem Leser vielmehr Denkanstösse und möglicherweise neue Einsichten in das Thema »Security Awareness« respektive »Mensch gemachte Sicherheit« im Unternehmen vermitteln – dies in einer Zeit, in der unter dem Eindruck eines radikalen Paradigmenwechsels im Bereich des Informationsschutzes um neue, tragfähige Konzepte gerungen wird.

Die Vielfalt, die Awareness inhärent ist, spiegelt sich im Aufbau des Buches wider. Da wird ein Blick auf die Sicherheitskultur geworfen (Kap. 2 und Kap. 5.3ff) und Awareness aus Sicht der Werbepsychologie (Kap. 4) betrachtet, ebenso wie aus der gestaltpsychologischen und tiefenpsychologischen Perspektive (Kap. 5). Es werden die kommunikationsrelevanten Erkenntnisse des klassischen Marketings (Kap. 4) behandelt wie auch die Sicht der integrierten und systemischen Kommunikation (Kap. 6). Auch wie man Sicherheit »lernen« kann (Kap. 3) und im Rahmen von Kampagnen interkulturellen Aspekten Rechnung trägt (Kap. 7) erfahren Sie in auf den folgenden Seiten.

Verständnis von Security Awareness

Dass Sicherheitskultur sich nicht nur über Produkte, Services und Branchenzugehörigkeit des Unternehmens, über Standorte oder dem Status des jeweiligen Sicherheitsverantwortlichen ausdrückt, sondern bereits im Verständnis von Security Awareness integriert ist, lässt sich aus den zahlreichen Ansätzen (s. Kap. 2.4, Kap. 5.4 und Kap. 5.9) ableiten, die mit dem Begriff bzw. dessen Definition verknüpft sind.

Denn der eine sensibilisiert, der andere macht »bewusst«, ein Dritter »wirbt« für mehr »Bewusstsein« oder »Aufmerksamkeit«. Für die einen sind Security Awareness Maßnahmen (fertige) »Programme«, die man quasi nur noch implementiert. Für den anderen eine »Marketing-Kampagne«, die strategisch geplant sein will und sich an kulturellen Bedingungen ausrichtet. Einer versteht unter Awareness Maßnahmen entlang einer klassischen Lerntheorie und schickt seine Mitarbeiter in Vorträge, Trainings, Workshops

oder – jeden für sich – zurück an seinen PC, damit er sich mit allerlei E-Learning-Tools (s. Kap. 3.3ff) beschäftigt. Ein anderer entdeckt die psychologisch geleitete systemische Kommunikation für sich und wirbt z.B. für »Empowerment« (s. Kap. 5.5) oder verteilt Giveaways zur »paradoxen Intervention« (s. Kap. 6.3.1). Manche laden Gratisposter und Flyer aus dem Internet und lancieren Security-Propaganda via Schwarzem Brett. Wieder andere investieren große Summen, um Filme, Hörspiele (s. Kap. 6.3.8) oder Spiele zum Thema und zur Begleitung von Prozessen (s. Kap. 6.4.2) entwickeln zu lassen. Vereinzelt gibt es da auch den CISO, der sich »Change« auf die Fahnen schreibt und seine Awareness als Veränderungsprozeß begreift. Doch Veränderungen einleiten kann nur derjenige, der sich selbst kennt (s. Kap. 5.1) und sich im Kontext Security Awareness also auch der Identität seines Unternehmens bewusst ist (s. Kap. 2.4 und 5.7).

Dritten wiederum ist es wichtiger, für sich selbst zu sorgen; sie positionieren sich, die Sicherheitsverantwortlichen, als Marke und scheinen sich sicher zu sein, dass sich so Awareness »en passant«, also von ganz allein, einstellt.

Einer unterteilt seine Kampagne in »Phasen«. Dem anderen ist das egal; er orientiert sich pragmatisch an aktuellen Entwicklungen, indem er seine Kommunikation den ganz realen Security-Phänomenen im Tages- und Wochenlauf des Unternehmensalltags anpasst. Oder aber er schafft Spannung und Involvement gerade über Brüche bzw. über eine eher fragmentarische Dramaturgie. Auch dann, wenn man nur einen der hier genanten Enabler von Awareness, die Psychologie, näher betrachtet, existieren selbst innerhalb dieser Facette sehr unterschiedliche Vorstellungen (s. Kap. 4 und 5).

Aufgrund dieser verschiedenen Auffassungen von Security Awareness ist dieses Buch auch als eine Bestandsaufnahme unterschiedlicher Awareness-Philosophien und –Bausteine zu betrachten und gleicht daher eher einem Handbuch. Neben der Darstellung der Einzelthemen aus den jeweils individuellen Perspektiven der Autoren und Autorinnen, von denen jede(r) für sich auch Expertisen aus ihrem Wirken im Kontext der Security Awareness beigetragen haben, werden in Kapitel 5, 7 und 8 zudem zahlreiche Praxisbeispiele, z.T. über Interviews mit den Sicherheits- bzw. Kampagnenverantwortlichen (Kap 7.8 und 8), in Wort und Bild präsentiert.

Insofern ist der Mix aus Theorie und Praxis, basierend auf den hier dargestellten Methoden und Beispielen als eine Einladung zu verstehen, Offensichtliches zu hinterfragen und die »versteckten« Phänomene hinter der bis heute überwiegend technologisch und organisatorisch geprägten Sicherheit zu entdecken.

München/Köln, im Juli 2009

Michael Helisch | Dietmar Pokoyski

Inhaltsverzeichnis

1 Security Awareness: Von der Oldschool in die Next Generation – eine Einführung

Dietmar Pokoyski

»Menschen tragen eigentlich immer die Schuld. Schließlich ist es der Mensch, der das Regelwerk entwickelt, das bestimmt. Doch viel interessanter ist die Frage: Wie oft haben Menschen beim Versagen technischer Systeme mit ihrer Kreativität Unfälle vermieden?« (Carsten Jasner/brand eins)

Der so genannte »Faktor Mensch« ist in den letzten Jahren zum Lieblingsargument einer bis dato technisch sozialisierten Security-Branche stilisiert worden. Die Menschen zu verstehen, sie zu erreichen und sie am Ende auch zu überzeugen, sie vielleicht zu verändern im Sinne einer gelebten und lebendigen Entwicklungsgeschichte, wird gerne als DER Erfolgsfaktor der Informationssicherheit dargestellt und der Security Awareness als primäre Aufgabe zugeschrieben.

Dabei gehört Security Awareness nach dem Verständnis vieler nicht selten zu den undankbarsten Dingen, denen man sich in Unternehmen widmen kann. Denn sie bereitet Arbeit, thematisiert u.a. paradoxe Handlungen, erzeugt sogar neue Risiken und der Erfolg ist – zumindest aus der betriebswirtschaftlicher Perspektive – aufgrund der beteiligten »weichen Faktoren«, schwerlich fassbar. Einerseits. Anderseits ist es wie immer, wenn man sich dem richtigen Leben stellt: ohne Blut, Schweiss und Dreck kein Weiterkommen und kein wirklicher Erfolg! Letztlich kommt kein Securitymanager daran vorbei, den von ihm verantworteten Unternehmensbereich weiter entwickeln zu wollen.

Obwohl die IT-orientierte Welt unsere Lehr- und Lernsysteme so ausgerichtet hat, als ob es darum ginge, Wissen praktisch downloaden zu wollen (Wielens 2008), wird sich auch die Securitybranche nicht länger um die tatsächliche Umsetzung hinsichtlich Faktoren jenseits von Technologie und Organisationslehre drücken können. Denn *»wer in der Evolution des Lebens mit ihren verrutschenden Zielen letztendlich überlebt, muss die Fähigkeit zum Spielen haben: Er darf sich nicht nur auf ein festes Ziel konzentrieren, sondern muss die Möglichkeit schaffen, verschiedenartigen zukünftigen Herausforderungen erfolgreich begegnen zu können. Dies verlangt Lebendigkeit, Flexibilität, Vermehrung von Optionen, anstatt Maximierung einer bestimmten Option.«* (Wielens 2008). Betrachtet man unseren Gegenstand aus einer derartigen, nahezu »sportlichen« Perspektive, so gibt es kaum ein anderes Thema, das sich facettenreicher gibt als Security Awareness.

Allerdings demonstrieren ja gerade Krisensituationen immer wieder, dass Options-Vielfalt zu den größten Lösungs-Bremsern in mitunter unbeweglich agierenden Chefetagen so mancher deutscher Unternehmen gehören. Und auch die relativ große Unsicherheit bezüglich einer klaren Definition von Security Awareness ist als eine mögliche Barriere bei der Entscheidung für Maßnahmen spürbar. Diese oft diffuse Wahrnehmung wird gerade auch in den Darstellungen durchgeführter wie auch aktueller Maßnahmen und Kampagnen deutlich. »Awareness« und »Bewusstsein« werden häufig als Synonym ver-

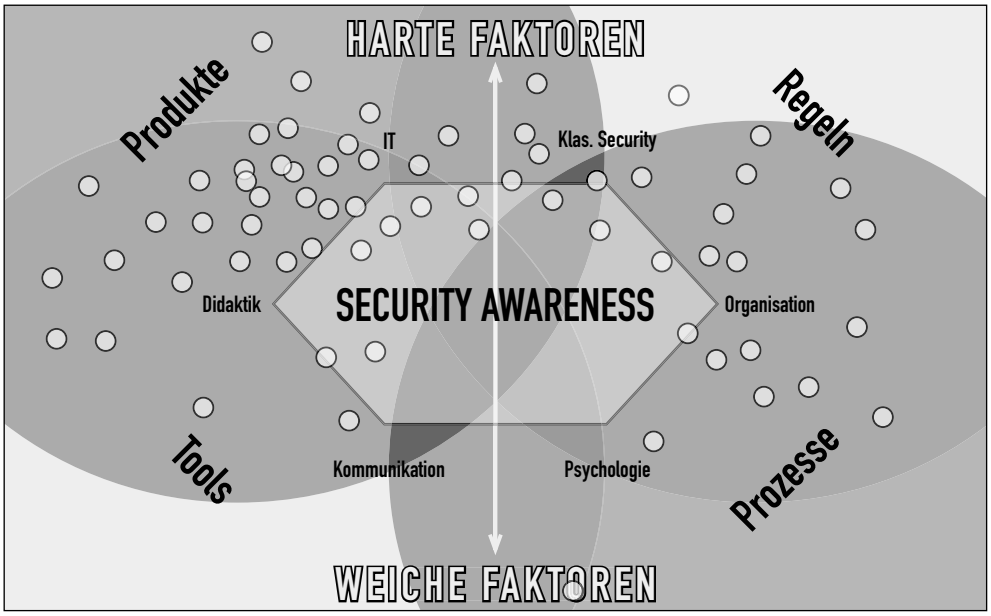

Abb. 1: Positionierungsmodell Anbieter und originäre Herkunft von Security Awareness Dienstleistern – je zentraler die Positionierung, um so stärker die Allrounder-Qualitäten des Anbieters (Quelle: known_sense 2009)

wendet. Es ist die Rede von »Sensibilisierung« und innerhalb Komposita erweitert um »Programme« und »Trainings«, etwa so, als könne man den Menschen Awareness wie eine Mütze oder einen Kopfhörer über das Haupt stülpen. Und als wäre das nicht schon verwirrend genug, zieht sich inzwischen auch der Begriff des »Empowerment«, der Awareness mit qualitativem Anspruch per se inhärent ist, durch die Fachmedien.

Der Security Awareness-Markt

Awareness mit oder ohne Empowerment – Sensibilisieren? Ermächtigen? Oder gar beides? Wer oder was hilft nun weiter? Wie finde ich z.B. den richtigen Awareness-Dienstleister? Inzwischen tummeln sich zahlreiche Anbieter mit z.T. sich überschneidenden, z.T. aber höchst unterschiedlichen Erfolgsmodellen auf dem Markt. Nicht nur, dass so ziemlich jedes IT-Beratungsunternehmen im Rahmen ihres Portfolios nice-to-have findet, auch Security-Awareness-Expertisen und -Konzepte anbieten zu können. Nein, selbst Wirtschaftsprüfer, Kanzleien oder Kommunikationsagenturen haben längst entdeckt, wie sich aus Unsicherheit in den Unternehmen und der Unsicherheit in Bezug auf den Begriff »Awareness« Kapital schlagen lässt.

Wer morgen eine Security Awareness-Kampagne angehen will, hat – je nach Strategie und Budget – heute die Wahl, seinen Dienstleister hinsichtlich Beratung und Produkt aus circa sechs Anbietergruppen zu wählen, deren Services sich mal mehr, mal weniger überschneiden und deren Protagonisten nicht selten miteinander kooperieren:

- große und mittlere IT- bzw. Technologiefirmen
- Beratungshäuser der IT- oder (klassischen) Sicherheitsbranche (oft auch zertifizierungs-, oder Audit-lastig)
- die bekannten »großen« Wirtschaftsprüfer bzw. Organisationsberatungen
- eher Produkt-getriebene Unternehmen mit Focus auf z.B. E-Learnings-Tools
- Hochschulen oder kleine innovative Research-Institute, z.T. mit psychologisch-sozialwissenschaftlichem Fokus
- Kommunikationsagenturen, die in der Regel individuelle Kampagnen kreieren, von denen einige wenige aber auch fertige Produkte oder Produktlinien wie z.B. Comics oder Giveaways lizenzieren

Darüber hinaus existieren auch etliche Anbieter kostenfreier Awareness-Tools, die Präsentationen bzw. Trainings- oder Learning-Einheiten, Print-Templates für Poster, Flyer o.a. klassische Medien, Videos oder Instant-Kontent fürs Intranet oder für Newsletter anbieten und aufgrund der in Regel minderen Qualität, vor allem aber wegen der »Neutralität« der angebotenen Tools (fehlende unternehmenskulturelle Anknüpfung) lediglich dann als seriös einzustufen sind, wenn sie den Anwendern nicht mehr als das berühmte Grundrauschen versprechen. An einen Mehrwert, etwa in Bezug auf Involvement oder gar eine potenziell beabsichtigte Verhaltensänderung, kann hier nur der Anwender glauben, der sich auch in seinem Job dem Rosenkranz verpflichtet fühlt oder aber Awareness für eine schnöde Pflichtveranstaltung hält.

Und selbst dann, wenn Sie die die Gratis-Tools rausfiltern und ebenso diejenigen, die in Ihren Service- oder Produktbeschreibungen mit unlauteren Bezeichnungen wie *»easy«*, *»einfach«* oder gar *»... ohne Beratung [...] in kürzester Zeit ...«* operieren, bleibt noch eine Vielzahl von Anbietern übrig, die vorgeben, tatsächlich Security Awareness betreiben zu wollen. Einer hat sich bei seiner Preisgestaltung offenbar beim Discounter um die Ecke inspirieren lassen und fordert *»Investieren Sie 99 Cent pro User [...] für die Schaffung eines Sicherheitsbewusstseins [...] als Bestandteil der Unternehmenskultur«*.

Billiger geht aber immer. So verspricht z.B. der Copytext einer im Awareness-Kontext angepriesenen Security-Management-Software u.a. *»...abc spart am Zeitaufwand: Die Teilnehmer brauchen nicht viel Zeit für die Tests [...] Der Sicherheitsbeauftragte braucht nicht viel Zeit zu investieren, um Untersuchungen zu entwickeln und zu organisieren ...«*. Wer sich darüber im Kontext Security Awareness verstanden und gut bedient fühlt, könnte zusätzlich auch über die Anschaffung eines Rosenkranzes nachdenken und den Heiligen Awareness-Geist um Unterstützung bitten. Denn hierbei handelt es sich wie bei vielen anderen ausschließlich Produkt-getriebenen Anbietern um nichts anderes als strategischer Opportunismus, indem den (verunsicherten oder allzu bequemen) Unternehmen exakt das gesagt wird, was diese (offensichtlich) hören wollen.

»...meiner Meinung nach ist die Security Awareness DIE Basis für eine gelebte Sicherheitskultur. Nach Pareto sind das in meinen Augen 80% des IS Gesamterfolgs.«

(Information Security Officer einer Internationalen Bank)

»Als Key Account Manager, die ganzheitliche IT-Nutzungskonzepte inklusive Services wie z.B. TÜV-zertifizierter Datenlöschung anbieten, diskutieren wir zunehmend mit unseren Kunden über Security Awareness. Aus meiner Sicht einer der spannendsten Themen im Lande des Exportweltmeisters.«

(Stephan Köhler, Key-Account Manager einer namhaften IT-Leasing-Firma)

»Ohne ein kultiviertes Sicherheitsbewusstsein greifen alle darüber liegenden Maßnahmen nur bedingt.«

(Christian Wahl, secunomic GmbH)

»... merke immer mehr, dass man Security-Probleme nicht allein durch Technik lösen kann.«

(Thomas Wallutis)

»... ein leider wenig beachtetes und doch sehr wichtiges Thema in der IT-Security ...«

(Jochen Mohr, Booster GmbH)

»Die Aufklärung und Sensibilisierung der Mitarbeitenden, sowie die klaren Richtlinien zu Umgang, Lagerung und Verfügbarkeit von Informationen bekommen immer mehr Gewicht.«

(Michael Linder, CASSARiUS AG)

»... befasse mich schwergewichtig mit ISMS und BCMS. In beiden Themenbereichen spielt das Verhalten von Menschen eine Schlüsselrolle. Awareness ist darum in verschiedenen Dimensionen ein zentrales Thema.«

(Martin Leuthold, InfoGuard AG)

»Awareness - eindeutig eines »meiner« Themen. Bei meinen internen Schulungen bin ich immer wieder verblüfft über die Unkenntnis und Naivität der Mitarbeiter in Bezug auf Unternehmenssicherheit.«

(n.b.)

»Awareness scheint mir eine notwendige geistige Voraussetzung, viel zu wenig verbreitet, ebenso wie dass, was bewirkt werden soll: Sicherheit. Und ich bin fest überzeugt, das dies aufgrund menschlicher Eigenschaften so ist, und genau nicht wegen technischer Unzulänglichkeiten.«

(Johannes Hubertz, hubertz-it-consulting GmbH)

»Vor allem die Sicherheitskultur liegt mir am Herzen, denn der Mensch ist und bleibt der größte Sicherheitsfaktor, sowohl in der Prävention wie auch in der Gefährdung.«

(Christian Riesen, Projektleiter IT, Wangen/Schweiz)

Abb. 2: O-Töne von Awareness-Gruppenmitgliedern eines populären Social Media-Netzwerkes

»Ich bin IT-ler und werde leider genau deshalb von den Anwendern häufig missverstanden, wenn ich das größte Sicherheitsrisiko circa 50 Zentimeter vor dem Bildschirm vermute. Sicherheit ist kein IT-Thema, kein technisches Thema. Solange die Risiken wie beim Rauchen einfach ignoriert werden, hilft keine Technik und keine Organisation. Awareness ist aus meiner Sicht der Schlüssel zur Sicherheit, und Awareness ist eine Frage der Kultur.«

(n.b.)

»Das Thema Awareness gehört für mich bei Betrieb und Anwendung zur ersten Grundausstattung!!!«

(Volker Jung, Siemens AG)

»Besonders interessiert mich das Thema »Awareness« durch die Hierarchieebenen, vom Administrator bis zum CEO. Mit einer Strategie? Meine Erfahrung ist hier: Besser zielgruppenorientiert.«

(n.B.)

»Der Mensch ist bei Sicherheitsfragen, also nicht nur bei IT-Sicherheit, der wichtigste Faktor. Und was viele nicht wahrhaben wollen: Er ist Erfolgsfaktor für Sicherheit, nicht nur Risikofaktor.«

(Thomas Faber, Landesinitiative secure-it.nrw)

»Benutzer-Awareness wird immer wichtiger, da allein durch technische Maßnahmen Informationssicherheit nicht gewährleistet werden kann.
Die IT in Unternehmen ist definitiv der falsche Ansprechpartner für Awareness (aber auch für Informationssicherheit (IS) generell). Leider liegt aber in der Realität die IS Aufgabe (noch immer) in der IT. Die Geschäftsleitung wäre der richtige Ansprechpartner, nur dort ist die Awareness für IS immer noch nicht angekommen. Hoffnung besteht allerdings, da ja Richtlinien und Gesetz genau in diese Richtung zielen. Nur bis zum Verständnis, dass BenutzerAwareness als (kostengünstiges) Mittel der Risikoverringerung eingesetzt werden kann ist es noch ein weiter Weg. Firewalls & IDS Systeme kann man angreifen, die haben Gewicht, da bekommt man kg für sein Geld. Awareness ist eine »weiche« Maßnahme, das »bringt nix«. Das Sicherheitskultur in die Firmenkultur integriert wird, muss vor allem die Geschäftsleitung vom Nutzen überzeugt sein. Da helfen ganz sicherlich auch Bücher.«

(Thomas Schnabl, Business Protection e.U.)

»As an information security professional I see one of the most important aspects in my daily job the culture and mentality of people, thus security Awareness is one of the most powerful weapon to raise or even create this culture and mentality.«

(Jean Goetzinger, CISO, Banque centrale du Luxembourg)

»Das Thema Awareness ist meine Lieblingsbaustelle im meinem geschäftlichen Umfeld.«

(Axel Hannappel, HANNAPPEL APPLIED SECUR(IT)Y e.K.)

»Security Awareness ist in der Tat die wichtigste Maßnahme um das Security Level entscheidend zu heben.«

(Rainer Rehm)

Es geht aber auch anders! Vielleicht kennen Sie die die alles überragende Streetworker-Sendung im deutschen Fernsehen, »Die Kochprofis«, und insbesondere die Episode 56? Mittendrin überreicht man dem Schweizer Campingplatz-Restaurant-Betreiber Ueli die von den zur Hilfe gerufenen Kochprofis relaunchte Speisekarte für seinen mehr als schlecht laufenden Betrieb. Ueli, der eigentlich froh sein müsste, seine qualitative Positionierung gegenüber den Campingkochern mit ihrem Dosenfraß zu verbessern, stellt aber kopfschüttelnd fest, dass die neue Karte so nicht funktionieren würde. Denn falls er, der Restaurant-Besitzer, als Koch einspringen müsste, bräuchte er eine exakte Anleitung, ob und zu welchem Zeitpunkt er Sack 1, Sack 2 oder Sack 3 (Anm.: gemeint sind die bis dahin verwendeten XXL-Fertigprodukt-Tüten) zu öffnen hätte.

Oldschool Awareness vs. Awareness 2.0?

Hier kommt in Abgrenzung zu den vielen Fertigprodukten der Oldschool Awareness die Awareness Next Generation ins Spiel, von dem in den folgenden Kapiteln häufig die Rede im sein wird – stets im Sinne eines idealen Awareness-Methoden-Mix. Denn während die klassische Schule trotz der nicht zu verleugnenden positiver Ansätze, zumindest eine Sättigung erzeugen zu wollen, vor allem auf Didaktik und hier insbesondere auf die klassische Lerntheorie bzw. Betriebswirtschaftslehre mit ihrem hohen Anteil an Convenience und Geschmackverstärkern setzt, möchte die Next Generation in dem Wissen um die dynamischen, prozess-orientierten Komponenten von Awareness mehr als nur den ersten Heißhunger auf sicheres Verhalten stillen. Sie möchte aus einem Fundus an zahlreichen erprobten und qualitativ hochwertigen Methodik-Zutaten nachhaltige Awareness-Menus erkochen – auch mit dem Ziel einer Corporate Health, die einhergeht mit der persönlichen wie gemeinschaftlichen Lust, sich und das jeweilige unternehmerische Umfeld nachhaltig zu schützen.

Diese Trennung ist eine methodische Trennung, denn auch die schlichte Sättigung, das Wissen um (respektive die Nutzung von) Basics der Oldschool gehören zu den Grundlagen der Awareness Next Generation – bilden also sozusagen einen kräftigen Fond, der nun noch verfeinert werden will.

In diesem Sinne orientiert sich Awareness Next Generation konsequent an …

- unternehmenskulturellen Aspekten und deren methodische Transformation in praktische Maßnahmen
- Blended Learning
- klassischen und innovativem Marketing
- integrierter und systemischer Kommunikation
- psychologischen Grundlagen und
- Changemanagement.

Denn der Schlüssel zur Security ist unterm Strich stets der Mensch. Ihn zu verstehen, ihn zu erreichen – und das nicht nur auf eine kognitive Art, sondern in dem Wissen um verdeckte Faktoren – und ihn am Ende auch zu überzeugen, ihn vielleicht zu VERÄNDERN im Sinne einer Entwicklungsgeschichte, ist die große Aufgabe der Awareness.

AWARENESS NEXT GENERATION stellt also nicht nur den Menschen in den Mittelpunkt ihrer Betrachtung; sie betrachtet menschliches Handeln sowohl aus individueller Sicht als auch aus systemischer Sicht des Sozialgefüges Unternehmen. AWARENESS NEXT GENERATION nutzt schließlich auch Methoden, die über eine größtmögliche Passung zum Gegenstand ihrer Betrachtung, den Menschen, verfügen. AWARENESS NEXT GENERATION heißt: state-of-the-art-Ansätze zu nutzen, die sich bereits in anderen Kontexten der oben genannten Felder bewährt haben. Heißt z.B., das Bewusstsein dafür zu entwickeln, dass etwa die Struktur von Kampagnen nicht zwingend modular eingeteilt werden muss. Und es kann u.a. auch bedeuten, dass eine Kampagne nicht nur aus einem Comic und der maximalen Diversifizierbarkeit hinsichtlich der Verwertung seiner Figuren bis hin zum Tassenaufdruck und anderen Merchandising-Artikeln besteht.

Auch weigert sich AWARENESS NEXT GENERATION beharrlich, in den Schlüsselapplikation der OLDSCHOOL, den Trainings und anderen didaktischen Präsenzveranstaltungen (s. Kap. 6.5) mit ihrem ausschließlichem Bezug zur Lerntheorie (s. S. 75f.) stecken zu bleiben. Denn mit Blick auf den Leistungssport würde auch niemand erwarten, dass ein einmaliges Training – selbst eine Handvoll – einen nachhaltigen Effekt zur Leistungssteigerung generiert.

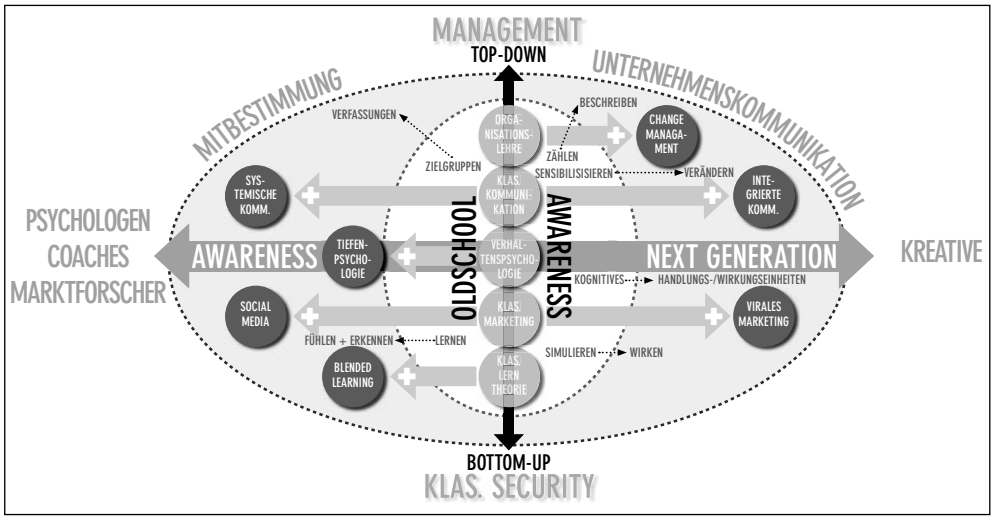

Abb. 3: Awareness Next Generation: Die eindimensionalen und vertikalen Top-Down- und Buttom-Up-Beziehungen der Oldschool werden zugunsten eines stärker in die Horizontale agierenden Modells erweitert, bei dem neben den relevanten Unternehmensbereichen vor allem auch der systemische Blick von Außen durch Experten verschiedener Fachrichtungen Erfolg und Nachhaltigkeit von Awareness-Maßnahmen sichert (Quelle: known_sense 2009)

Awareness Next Generation definiert zudem den Begriff der Zielgruppen neu. Neben Bildung, Status in der Unternehmenshierarchie, der Zugehörigkeit zu bestimmten Organisationseinheiten oder der funktionalen Rolle setzt es auf Verfassungsmarketing, das davon ausgeht, dass Mitarbeiter ihr Verhalten – je nach Stimmung, in der sie sich gerade befinden – verändern. Ein professionelles Awareness Marketing macht daher situative Verfassungen im Sinne von Befindlichkeiten, Metaphern oder Erlebniswelten zum psychologischen Trigger der Mediennutzung, denn sie sind die wirklichen Bezugspunkte von Kampagnen, die Anbindung an die Menschen sucht.

Zwar nutzt Awareness Next Generation auch quantitative Erfolgsmessungen, dies jedoch nicht in blindem Vertrauen auf die statistische Aussagekraft von Zahlen. Vielmehr setzt sie ebenso auf Verfahren, mit denen verdeckte Ursachen beschrieben werden können – mithin auf qualitative Ansätze wie z.B. der Wirkungsforschung (s. Kap. 5.2ff).

Kurz: Awareness Next Generation redet nicht nur über Menschen oder stellt Ihre Eigenschaften und Ausprägungen in Zahlen dar, sie tut auch etwas für sie.

Wir sprechen dann von Awareness Next Generation, …

- wenn die Awareness-Maßnahmen im Unternehmen strategisch – d.h. unternehmenskuturell – unterfüttert implementiert werden.
- wenn das mit Security Awareness-Maßnahmen einhergehende Veränderungsmanagement den ausgelösten Prozessen interaktiv begegnet, d.h. die Menschen in einen Dialog miteinander verwickelt.
- wenn in diesem Rahmen auf methodisch fundierte, weil erprobte Methoden und Ansätze (z.B. Konsumenten- und Wirkungsforschung, Verfassungsmarketing, etc.) zurückgegriffen wird.
- wenn in punkto Kommunikation die werblichen Möglichkeiten nicht mit den klassischen Medien ausgeschöpft sind und Marketing-Kampagnen – je nach Strategie – neue Wege suchen, um einen qualitativen Kontakt zu den Menschen zu finden (z.B. Guerilla Marketing, Blended Learning, Social Media, etc.).
- wenn es zu den Zielen gehören, die Identifikation der Mitarbeiter mit dem Unternehmen und die Loyalität gegenüber dem Unternehmen zu thematisieren.

Gerade Loyalität ist keine Eigenschaft, die trainiert werden oder ausschließlich über Kommunikation erzeugt werden kann. Identifikation und Loyalität bedeuten Geben und Nehmen. Dieses Geben und Nehmen ist dabei aber nicht auf den Rahmen der rein betriebwirtschaftlichen Austauschbeziehung »Arbeitsleitung gegen Entlohnung« beschränkt, sondern lässt dies vielmehr links wie rechts stehen. Denn Identifikation und Loyalität gehen einher mit Verantwortung und Verantwortung mit einem Beteiligt-Sein. *»Ich schütze quasi aus mir selbst heraus, was mir lieb und teuer ist, weil ich es so will«* – so einfach könnte Awareness auch sein.

2 Definition von Awareness, Notwendigkeit und Sicherheitskultur

Michael Helisch

2.1 Was hat es mit Awareness auf sich?

2.1.1 Awareness und Bewusstsein

Security Awareness findet seine begriffliche Entsprechung im Terminus Sicherheitsbewusstsein bzw. in der Umschreibung: »Ein Bewusstsein für das Thema Sicherheit entwickeln.« Was aber ist das Bewusstsein? Ein Blick in Wikipedia zeigt, dass Bewusstsein eine Vielzahl von Bedeutungen haben kann:

1. **Bewusstsein als »belebt-sein« oder als »beseelt-sein«** in verschiedenen Religionen oder als die unbegrenzte Wirklichkeit in mystischen Strömungen.
2. **Bei Bewusstsein sein:** Hier ist der wachbewusste Zustand von Lebewesen gemeint, der sich unter anderem vom Schlafzustand oder von der Bewusstlosigkeit abgrenzt. In diesem Sinn lässt sich Bewusstsein empirisch und objektiv beschreiben und teilweise eingrenzen. Viele wissenschaftliche Forschungen setzten hier an; insbesondere mit der Fragestellung, inwieweit das Gehirn und das Bewusstsein zusammenhängen.
3. **Bewusstsein als phänomenales Bewusstsein:** Ein Lebewesen, das phänomenales Bewusstsein besitzt, nimmt nicht nur Reize auf, sondern erlebt sie auch. In diesem Sinne hat man phänomenales Bewusstsein, wenn man etwa Schmerzen hat, sich freut, Farben wahrnimmt oder friert. Es wird allgemein anerkannt, dass Tiere mit hinreichend komplexer Gehirnstruktur ein solches Bewusstsein haben. Phänomenales Bewusstsein ist als so genanntes Qualiaproblem eine Herausforderung für die naturwissenschaftliche Erklärung.
4. **Bewusstsein als gedankliches Bewusstsein:** Ein Lebewesen, das gedankliches Bewusstsein besitzt, hat Gedanken. Wer also etwa denkt, sich erinnert, plant und erwartet, dass etwas der Fall ist, hat ein solches Bewusstsein. Es ist als Intentionalitätsproblem eine Herausforderung für die naturwissenschaftliche Erklärung.
5. **Bewusstsein des Selbst und seiner mentalen Zustände:** Selbstbewusstsein in diesem Sinne haben Lebewesen, die nicht nur phänomenales und gedankliches Bewusstsein haben, sondern sich auch darüber im Klaren sind, dass sie ein solches Bewusstsein haben. Dieses Selbstbewusstsein ermöglicht somit ein Bewusstsein von sich selbst als Individuum. Man trifft es bei Menschen und rudimentär bei einigen Säugetieren an.

6 **Individualitätsbewusstsein** besitzt, wer sich seiner selbst und darüber hinaus sich seiner Einzigartigkeit als Lebewesen bewusst ist und die Andersartigkeit anderer Lebewesen wahrnimmt.

Aufgrund dieser Bedeutungsvielfalt existiert zum einen keine allgemeingültige Definition von Bewusstsein. Zum anderen muss der Begriff Bewusstsein immer im jeweiligen Kontext betrachtet werden, auf den er sich bezieht. So ist, wie sich in Wikipedia nachlesen lässt, das Phänomen des Bewusstseins eines der größten ungelösten Probleme der Philosophie sowie der Naturwissenschaft, während im Bereich der Psychologie Klärungsansätze vorhanden sind (siehe hierzu auch die Definition Security Awareness aus Sicht von Gestaltpsychologie in Kap. 5.1.1 bzw. aus Gestalt- und Tiefenpsychologie, Kap. 5.9).

2.1.2 Security Awareness: Ein Begriff – viele Interpretationen

Security Awareness zeichnet sich durch eine Vielfalt an Interpretationsmöglichkeiten aus. So bezieht mancher Awareness lediglich auf die Gefahren im Umgang mit dem Internet. Andere wiederum sehen Awareness in einem direkten Bezug zu IT-Sicherheit oder datenschutzrechtlichen Fragestellungen. In weiten Fassungen wird Awareness im Kontext der Informationssicherheit oder des Risikomanagements gesehen. Letztendlich bestimmt die unternehmensindividuelle Realität, welche Themen von den jeweils Verantwortlichen darunter subsumiert werden. Hinsichtlich des Bezugsobjekts von Security Awareness gibt es somit kein RICHTIG oder FALSCH, denn entscheidend ist auch hier der jeweilige Kontext, auf den sich Awareness-Maßnahmen beziehen. Bei der begrifflichen Abgrenzung hilft möglicherweise ein Perspektivwechsel, mithin die Definition des Begriffs Awareness aus der Sicht der von Sicherheitsmaßnahmen »Betroffenen«. Welche Themen bzw. Aspekte hat Sicherheit aus dem Blickwinkel der Anwender?

Allzu oft wird Awareness ausschließlich in einem Atemzug mit dem Begriff Training genannt (vgl. hierzu auch Kap. 3). Zwar beeinflusst die Art und Weise, wie Wissen vermittelt wird, den Erfolg von Awareness-Aktivitäten. Menschliches Verhalten ist allerdings nicht allein rational bedingt, weshalb es zu kurz gegriffen wäre, reduzierte man Awareness ausschließlich auf den Faktor Wissen.

> *»Training is formal, having a goal of building knowledge and skills to facilitate the job performance. … Training strives to produce relevant and needed security skills and competencies.«*
>
> *»Awareness is not training. The purpose of Awareness is simply to focus attention on security. …Awareness is intended to allow individuals to recognize security concerns and respond accordingly. …Awareness relies on reaching broad audiences with attractive packaging techniques.«* (Wilson und Hash 2003)

»Awareness ist Einstellungssache« – dieses Statement wird gern und oft verbreitet. Awareness ist in der Tat auch Einstellungssache, aber eben NICHT NUR Einstellungssache. Um die vorhandene Einstellung eines Menschen zu verändern und sie in Hinblick auf

ein bestimmtes Ziel auszubilden, kommen neben dem Faktor Training (Kap. 3), Marketingkommunikation (Kap. 4 und 6) und Psychologie (Kap. 4 und 5) ins (Awareness-)Spiel. Beide Faktoren geben wichtige Antworten darauf, warum Menschen so handeln wie sie handeln und wie darauf zu reagieren ist. Im Kontext von Awareness liefern sie wichtige Hinweise für das Modellieren von Botschaften, den Einsatz und die Gestaltung von Awareness-Tools und -Medien (s. Kap. 6.3ff) mit denen definierte Zielgruppen erreicht werden sollen.

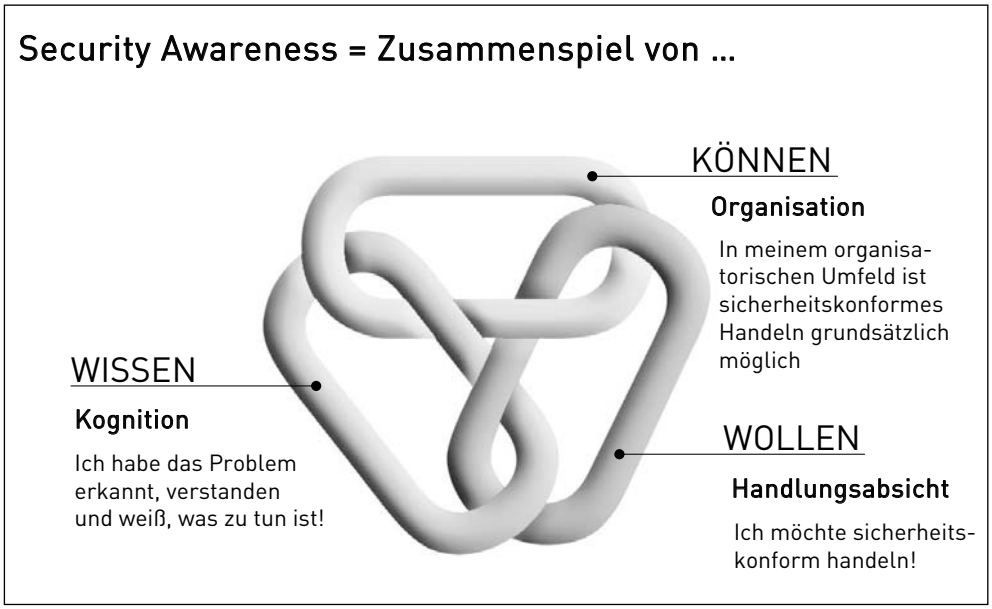

Abb. 4: Security Awareness = Zusammenspiel von Können, Wollen und Wissen

Security Awareness ist bekanntlich eine nie endende Aufgabe, ein stetiger Prozess. Diesem Prozess immanent ist Veränderung (vgl. Auch Kap. 5.1). Veränderung bei den von Awareness betroffenen Menschen – sei es in der Rolle des Mitarbeiters oder als Privatperson. Damit aber auch Veränderung in den Unternehmen selbst, in denen Menschen als Mit-Arbeiter ihre tägliche Arbeit verrichten und gleichzeitig sicherheitskonform handeln sollen. Das tun sie in den seltensten Fällen allein, sondern vielmehr interagierend mit anderen »Mit-Arbeitern«, was Awareness zunehmend komplex macht. Im Unternehmen als komplexes Organisationsgebilde müssen die Mitarbeiter aber die Chance haben, das nach einer Awareness-Kampagne erworbene Sicherheitswissen sowie die Motivation, sicher handeln zu wollen, in ihrem Arbeitsumfeld dauerhaft und nachhaltig ein- und umsetzen zu können. Das kann und wird sinnvoll nur funktionieren, wenn der organisatorische Rahmen, in dem sie Tag für Tag an vielerlei Themen mitarbeiten, passt. Determiniert wird dieser Rahmen durch die unternehmensindividuelle und -kulturelle Ausgangslage, die Vision bzw. die zu erreichende Ziel-Situation sowie durch das strategische und operative Vorgehen bei der Umsetzung. Dieser Veränderungsprozess will also

systematisch geplant, professionell begleitet und ebenso umgesetzt werden. Je nach Ausmaß der Veränderung bedeutet dies mehr oder weniger Aufwand.

> *»Change capability is necessary for the organizations that will succeed in the future. Effective communication, full and active executive support, employee involvement, organizational planning and analysis and widespread perceived need for change are the big five when successful change is achieved.«* (Heathfield 2008)

Bei hinreichender Größe des Awareness-Vorhabens sollte es in einem eigenen Projekt gemanaged werden. Was bedeutet hinreichend? Allein schon die Tatsache, dass ein solches Vorhaben die Zusammenarbeit mehrerer Personen aus möglicherweise unterschiedlichen Organisationseinheiten und/oder aus verschiedenen Standorten erforderlich macht, begründet das Aufsetzen eines Projektteams. Awareness-Aktivitäten bestehen meist aus einem Verbund von Maßnahmen. Jede einzelne Maßnahme muss für sich geplant und deren Umsetzung gesteuert werden. Damit die einzelnen Maßnahmen auch im Verbund den gewünschten Effekt erzielen, bedarf es ihrer übergeordneten Abstimmung. Auch an dieser Stelle entsteht Planungs-, Steuerungs- und Koordinationsaufwand. Glücklich kann sich das Unternehmen schätzen, das bei einem solchen Vorhaben auf einen übergeordneten »Kümmerer« zurückgreifen kann, der Prozesse, Termine und Ressourcen stets im Auge behält. Selbst bei extern eingekauften »Standard-Awareness-Lösungen« bleibt immer noch die Aufgabe, diese an die konkrete Situation im Unternehmen anzupassen. Auch das ist selten ein Selbstläufer.

In der Realität wird Awareness oft nur auf die Schlagworte Marketing und/oder ausschließlich nur auf den Begriff Training reduziert. Diese Reduktion wird der in der Realität nun mal vorliegenden Komplexität der Einflussfaktoren menschlichen Verhaltens aber nicht gerecht. Diesbezüglich werden die Kapitel zu den Teilaspekten Didaktik, Psychologie, Kommunikation und Marketing ein wenig mehr »Licht ins Dunkel« bringen. Auf die eingangs dieses Kapitels gestellte Frage: »Wie weit geht Security Awareness?« gibt es somit keine allgemeingültige Antwort. Awareness schließt aus meiner Sicht all' das ein, was menschliches Verhalten im Unternehmen und im Umgang mit sicherheitsrelevanten Informationen im Speziellen beeinflusst.

2.2 Relevanz von Awareness

»Each participant is an important actor for ensuring security.« (OECD 2002)

Awareness macht einerseits Arbeit, andererseits ist der ROSI (return on security invest) im Kontext Awareness mangels eindeutiger Messbarkeit nur schwerlich nachweisbar. Was also tun? Einfach so weitermachen wie bisher? Abwarten, bis etwas passiert, in der Hoffung, dass nichts passiert? Falls etwas passiert, einfach den Ursachen auf den Grund gehen und daran arbeiten? Warum, so die berechtigte Frage, sollte man sich den mit Awareness verbundenen Aufwand freiwillig aufhalsen? Die Antwort darauf ist simpel: Wo der Mensch intervenierend in sicherheitsrelevante Prozesse oder Arbeitsabläufe ein-

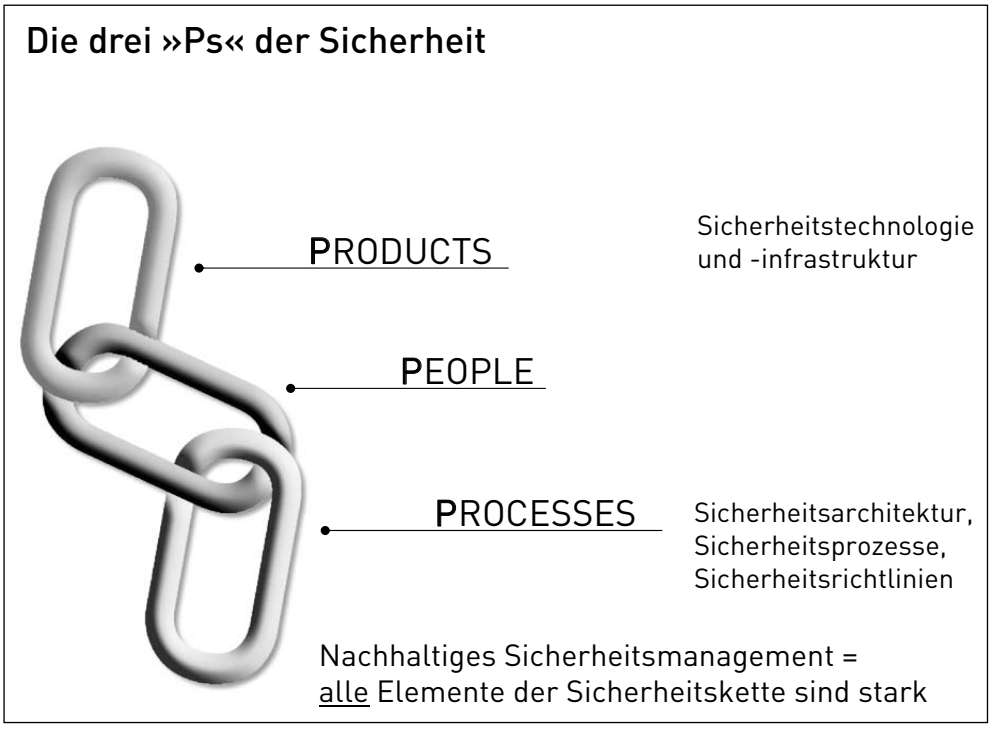

Abb. 5: Modell der drei »Ps« der Sicherheit von HECOM Security Awareness Consulting

wirkt, ist er automatisch Teil der Sicherheitskette. Dabei muss jedes Glied dieser Kette stark sein, sonst wird sie den ihr zugedachten Zweck, Sicherheit zu gewährleisten, nicht erfüllen können. Wer also ein nachhaltiges Risiko- bzw. Sicherheitsmanagement anstrebt, der kommt an der Einbeziehung des »Faktors Mensch« nicht vorbei.

Meiner Auffassung nach sind für ein nachhaltiges Sicherheits- und Risikomanagement drei »Ps« essentiell. Dabei handelt es sich zum einen um die Produkte, also den gesamten technischen Teil d.h. Sicherheitstechnologie, -infrastruktur, Hard- und Software, etc. Zum anderen geht es um die Prozesse, also den strategisch-konzeptionellen Sicherheitsrahmen inklusive der Sicherheitsarchitektur, Richtlinien und Standards. Zentrales Bindeglied zwischen Produkten und Prozessen ist der Mensch. Er ist derjenige, der die ihm zur Verfügung gestellte technische Infrastruktur richtig bzw. zweckmäßig bedienen soll, er ist zugleich derjenige, der die definierten Prozesse leben soll.

2.2.1 Informationen als schützenswerte betriebliche Assets

Mit dem Übergang von der industriellen Gesellschaft zur Wissensgesellschaft stellen Wissen und Innovation zunehmend die zentralen Objekte der Wertschöpfung dar. Wissen ist mittlerweile zum vierten Produktionsfaktor geworden. Jedoch: Kein Wissen ohne Informationen. Information ist unabdingbare Ressource im Leistungserstellungspro-

zess, gleichsam wesentlicher Faktor für erfolgreiches unternehmerisches Handeln. Sie ist die Basis für unternehmerische Entscheidungsprozesse, denn ohne Information keine (sinnvolle) Entscheidung. Informationen sind zugleich ein wesentlicher Wettbewerbsfaktor. »Wissen ist Macht« – wem ist dieses geflügelte Wort nicht bekannt? Wissen und Information ist nicht nur Macht – vielmehr begünstigen Wissensvorsprünge (Markt-) Macht. Informationen haben jedoch ambivalenten Charakter. Sinnvoll und nachhaltig geschützt sind sie ein Faktor für betriebswirtschaftlichen Erfolg, ungeschützt werden sie zu einem unternehmerischen Risiko. Informationen sind somit ein schützenswertes Gut. Die dauerhafte Sicherstellung der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Informationen sowie des Datenschutzes haben sich in diesem Kontext als weithin anerkannte Schutzziele der Informationssicherheit etabliert. Die Gewährleistung von Sicherheit und Datenintegrität – insbesondere bei elektronischen Transaktionen – beeinflussen nicht zuletzt Kundenbindung und Kaufverhalten. Allein der Anschein nur mäßig geschützter Informationen bzw. IT-Struktur kann negative Folgen für das Image und den Umsatz eines Unternehmens haben. Hier nachhaltig vorzubeugen ist nicht nur das Gebot der Stunde, sondern verpflichtet viele Unternehmen für ihr eigenes, zukünftiges Handeln. Vorbeugen bedeutet, über eine technische Infrastruktur zu verfügen, die Schritt hält mit den Risiken, das strategische Vorgehen in Sachen Sicherheit zu definieren, Sicherheitsprozesse und -richtlinien zu erstellen, diese kontinuierlich und gemäß den sich im Zeitablauf verändernden Risikoeinschätzungen zu pflegen und daraus eine adäquate Sicherheitsmaßnahmenplanung abzuleiten.

Die Einsicht in die Notwendigkeit technischer Vorsorgemaßnahmen ist im Markt weit verbreitet vorhanden. Mit der Einsicht in die Notwenigkeit strategischer Sicherheitsüberlegungen sowie der Einsicht in die Definition und laufende Anpassung risikoadäquater und gleichzeitig klarer Prozesse ist es im Vergleich zu den technischen Vorsorgemaßnahmen allerdings nicht ganz so gut bestellt. Dieser Sachverhalt wird auch durch die <kes>/Microsoft-Sicherheitsstudie 2008 bestätigt. Dort heißt es: »*Über ein Drittel der teilnehmenden Organisationen hat nach wie vor keine schriftliche Strategie zur Informationssicherheit. […] Klare Policies sind weiterhin keine Selbstverständlichkeit, nicht einmal in der sicherheitsbewussten Zielgruppe der Studienteilnehmer! […] Auch schriftlich formulierte Maßnahmen sind erneut in der Gunst gefallen und nunmehr nur noch bei 52 % (-5 Prozentpunkte) der Teilnehmer vorhanden (2006: 57%, 2004: 65%).*« (<kes>/Microsoft Sicherheitsstudie 2008)

Substantieller Nachholbedarf besteht bis dato immer noch beim »Faktor Mensch«. Zwar ist zu beobachten, dass man in jüngster Zeit häufiger bereit ist, dem Thema Gehör zu schenken, dennoch: Der Mensch wird in der betrieblichen Realität als Sicherheitsfaktor leider (noch) zu häufig vernachlässigt. Somit sind nicht ALLE relevanten Elemente der viel zitierten Sicherheitskette stabil. In der Konsequenz bedeutet dies, dass ein ganzheitliches, die relevanten Risikofaktoren integrierendes Sicherheitsmanagement in der Praxis eher die Ausnahme als die Regel darstellt. Gerade vor dem Hintergrund der zuvor erwähnten Ambivalenz von Informationen ist der Faktor Mensch aber kein unbedeutender. Je nachdem, welches Verhalten er im Umgang mit der IT-Infrastruktur und damit mit

seinen eigenen oder den Informationen des Unternehmens an den Tag legt, wird er zu einem Risikofaktor oder einem entscheidenden Instrument zur Risikominimierung.

2.2.2 Weitere Treiber für Awareness

»Es braucht zwanzig Jahre, um sich ein Ansehen aufzubauen, aber nur fünf Minuten, um es zu ruinieren.«
(Warren Buffett, Amerikanischer Investor und Geschäftsmann)

Der Handlungsdruck, den die Rechtsprechung auf Geschäftsführer und Vorstände ausübt, hat in den letzten Jahren deutlich zugenommen (IDC 2006). Am deutlichsten ist dies im Bereich der Banken und Versicherungen zu beobachten. Nationale (z.B. MaRisk, § 93,3 AktG, KonTraG, Verschärfung der Organhaftung lt. UMAG) wie auch internationale Bestimmungen (z. B.: Basel II, Sarbanes-Oxley Act of 2002) erhöhen in diesem Sektor die Anforderungen an das Risikomanagement und damit einhergehend auch an die Informationssicherheit. Sensibilität für Informations-Risiken sowie einen risikoadäquaten Umgang mit diesen fordern zunehmend auch Rating-Agenturen von börsennotierten Unternehmen bzw. Kreditinstitute von ihren Firmenkunden im Rahmen des internen Rating-Prozesses.

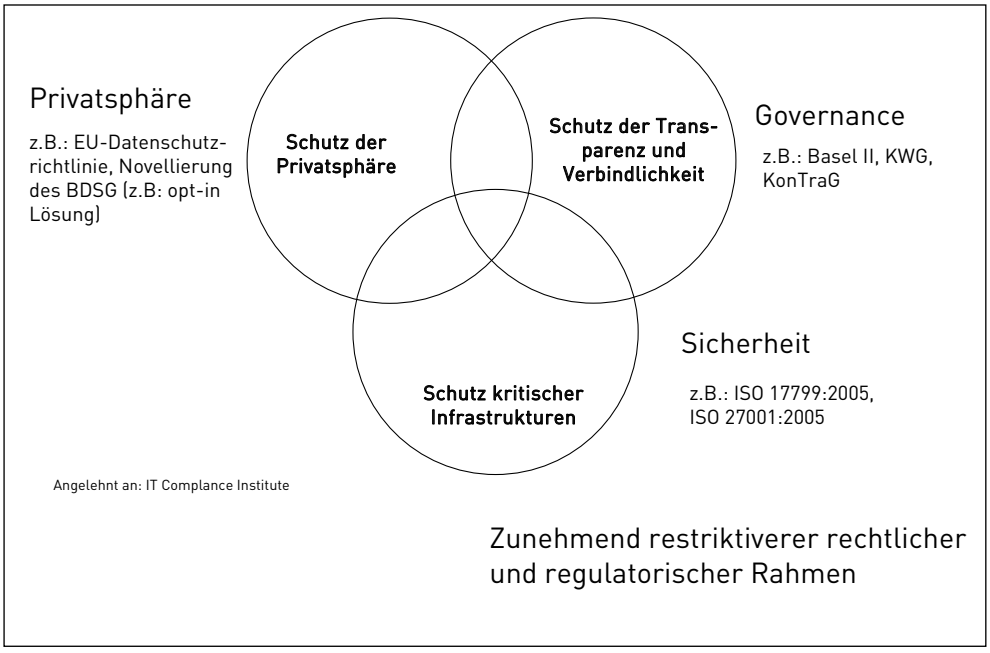

Abb. 6: Sicherheit im Kontext Governance und Schutz der Privatsphäre

Klassische Bedrohungen wirken ebenfalls als Treiber für Awareness. Hier ist festzustellen, dass diese in den letzten Jahren stetig zugenommen haben. So berichtet beispiels-

weise die Firma IKARUS Software, dass sich die Anzahl der täglich neu registrierten Malware Codes in 2008 im Vergleich zum Vorjahr von 8.800 auf durchschnittlich 31.000 verdreifacht hat (IKARUS 2009). Bereits im Jahr 2007 hatte sich die Zahl neu entdeckter Malware verdoppelt – es wurden so viele Schadprogramme verbreitet, wie in Summe in den vergangenen 20 Jahren (F-Secure 2008). Zu beobachten war in 2008 laut Ikarus auch eine Spezialisierung hin zu »intelligenten« Attacken mit immer ausgefeilteren Tarnfunktionen (IKARUS 2009). Da verwundert es nicht, dass *»Cybercrime ... der am schnellsten wachsende Wirtschaftszweig in der IT-Industrie ist«* (Chip-Online 2008). Die Relevanz von Malware als Risikotreiber Nr.1. bestätigt auch die <kes>-/Microsoft-Sicherheitsstudie 2008.

Risikosituation

Gefahrenbereich	Bedeutung		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	bei
Malware	1	1,12	1	1,19	4	21%
Irrtum und Nachlässigkeit eigener Mitarbeiter	2	0,93	2	0,79	1	36%
Hacking (Vandalismus, Probing, Missbrauch,...)	3	0,59	3	0,77	8	11%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	4	0,55	4	0,71	7	12%
Software-Mängel-/Defekte	5	0,54	5	0,49	3	26%
Hardware-Mängel-/Defekte	6	0,45	9	0,28	2	34%
Mängel der Dokumentation	7	0,40	10	0,27	6	15%
unbeabsichtigte Fehler von Externen	8	0,36	8	0,34	5	16%
Sabotage (inkl. DoS)	9	0,36	6	0,46	10	6%
Manipulation zum Zweck der Bereicherung	10	0,34	7	0,38	9	8%
höhere Gewalt (Feuer, Wasser, ...)	11	0,25	11	0,15	11	4%
Sonstiges	12	0,06	12	0,01	12	2%

Abb. 7: ‹kes›/Microsoft-Sicherheitsstudie 2008

Indirekte Treiberfunktion für Awareness üben auch die Sicherheitsvorfälle aus, die 2008 breite Medienpräsenz erfahren haben. Zu den spektakulären Fällen dieses Jahres gehörten u.a. (Computer-Zeitung 2008):

- Verlust von Adressen, Sozialversicherungsnummern und Bankdaten von 25 Mio. Briten
- Verlust eines Laptops, auf dem Personaldaten von 600.000 Angehörigen des britischen Militärs gespeichert waren, darunter Pass- und Versicherungsnummern sowie teilweise Bankverbindungen
- Pentagon: Unmengen an Daten und Passwörtern ausspioniert
- Supermarktkette TJX: 45 Millionen Kreditkartendaten ausspioniert
- Datendiebstahl bei Googles Outsourcing-Provider

- Rechner mit Patientendaten der psychiatrischen Klinik der LMU auf dem Flohmarkt verkauft
- Verbraucherzentrale Schleswig-Holstein: CD mit über 17.000 Datensätzen mit Namen, den vollständigen Adressen mit Telefonnummern, Geburtstagen und den kompletten Bankdaten zugespielt
- Bundesregierung kommen 500 Rechner abhanden
- Verbraucherzentrale Bundesverband erwirbt sechs Millionen Datensätze für 850 Euro, vier Millionen davon mit zugehörigen Kontoinformationen
- PWC: 56.000 E-Mail Adressen inklusive zugehöriger Passwörter im Internet frei zugänglich
- Zugangsdaten von 208.000 Webseiten in den Händen von Hackerbanden
- Datenskandal bei T-Mobile: Mehr als 17 Millionen Kundendaten geklaut
- Telekom: Erneute Datenpanne
- Telekom: Adresshändler und Callcenter verschaffen sich Zugriff auf Namen, Adressen, Vertragsdaten und Bankverbindungen von mehreren tausend Festnetz kunden

Bereits im Lagebericht 2007 konstatiert das Bundesamt für Sicherheit in der Informationstechnik »einen massiven Handlungsbedarf in allen gesellschaftlichen Gruppen. Die Sicherheitskompetenz, so urteilen die Experten, *»[...] müsse auf allen Ebenen entscheidend verbessert werden.«* (Bundesamt für Sicherheit in der Informationstechnik 2007) Der Gesetzgeber hat darauf reagiert und die Anforderungen an das Risk-Management in Unternehmen erhöht, um Schadenspotentiale für ein Unternehmen, dessen Kunden und Partner zu minimieren. So beziffert beispielsweise das FBI das jährliche kumulierte Schadensvolumen allein aus Viren und Spyware-Angriffen für die betroffenen US-Unternehmen auf 54 Mrd. Euro. Die Schadenshöhe für die betroffenen US-Privathaushalte lag zuletzt

Folgende Kriterien sind...	sehr wichtig	wichtig	unwichtig	Vergleichzahl*	Vergleichs-zahl 2006*	Vergleichs-zahl 2004*
Verstöße gegen Gesetze/Vorschriften/Verträge	50%	44%	6%	1,44	1,46	1,40
Imageverlust	51%	41%	8%	1,42	1,36	1,35
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	46%	45%	9%	1,38	1,28	1,26
Verzögerung von Arbeitsabläufen	38%	53%	9%	1,29	1,31	1,21
Schaden bei Dritten/Haftungsansprüche	34%	54%	12%	1,22	1,28	1,27
indirekte finanzielle Verluste	37%	43%	21%	1,16	1,12	1,14
Verstöße gegen interne Regelungen	13%	68%	19%	0,94	0,89	0,72
direkter finanzieller Schaden an Hardware u.ä.	13%	63%	24%	0,88	0,95	0,75

Basis: Ø 132 Antworten

*Vergleichszahl errechnet aus sehr wichtig = 3, wichtig = 1, unwichtig = 0

Abb. 8: Risiken aus der <kes>/Microsoft-Sicherheitsstudie 2008

** errechnet aus einer Kombination der Einstufung nach Wichtigkeit (sehr wichtig, wichtig, weniger wichtig)*

bei 747 Mio. Euro (Monitoring Informationswirtschaft 2006). Welche Schadensszenarien bzw. Risiken lassen sich hier exemplarisch ableiten?

Neben dem zunehmenden gesetzlichen Druck, der unverminderten Relevanz klassischer Bedrohungen (Malware), der Tatsache, dass Sicherheitsvorfälle, wenn auch unfreiwillig, immer häufiger öffentlich wirksam werden, sowie aufgrund der oben geschilderten Schadensszenarien leitet sich die Relevanz von Awareness aus dem »Faktor Mensch« selbst ab.

Die <kes>-/Microsoft-Sicherheitsstudie 2008 führt Irrtum und Nachlässigkeit der eigenen Mitarbeiter auf Position zwei aller Gefahrenbereiche. Gemäß der in Abb. 7 Risikosituation aufgeführten Prognose wird dieser Faktor, was seine Bedeutung unter den wichtigs-

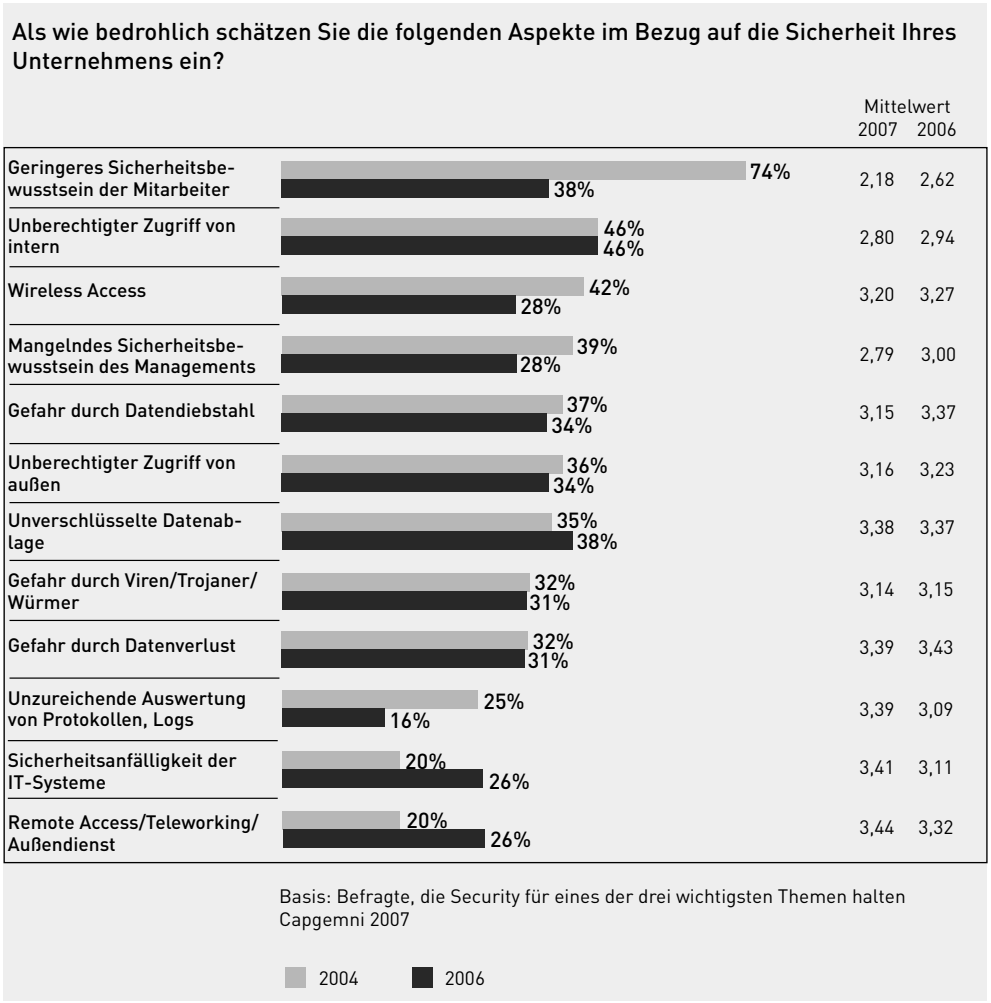

Abb. 9: Security Sorgen aus der Capgemini-Studie »IT-Trends« 2007, S. 19