Security Awareness-Kampagnen

Dirk Fox, Sven Kaun[1]

Kurzfassung:

In wachsendem Maße rückt – aus gutem Grund – die Sensibilisierung der Nutzer in den Fokus der Informationssicherheit. Zahlreiche Unternehmen haben Maßnahmen ergriffen, um ihre Mitarbeiter zu einem angemessenen Umgang mit den ihnen anvertrauten Informationen und der Informationstechnik anzuleiten und zu motivieren. Da diese Maßnahmen auf Einstellungs- und Verhaltensänderungen der Mitarbeiter zielen, reichen isolierte Einzelaktionen in der Regel nicht – erst eine systematische Bündelung eines „bunten", thematisch fokussierten Maßnahmenmixes unter dem Dach einer „Security Awareness Kampagne" zur Ansprache der Mitarbeiter auf unterschiedlichen (Kommunikations-) Ebenen kann diesen Anspruch erfüllen. Der Beitrag gibt einen Überblick über die Erfahrungen aus zahlreichen Awareness-Kampagnen in mittelständischen und großen Unternehmen.

Stichworte: Sensibilisierung für IT-Sicherheit, Awareness

1 Einleitung

Die Bedrohung von IT-Infrastrukturen hat sich in den vergangenen fünf Jahren exponentiell entwickelt. Wie aktuelle Zahlen zeigen, explodierten sowohl die Zahl der entdeckten Sicherheitslücken in verbreiteten IT-Systemen (Abb. 1) als auch die Anzahl neuer Viren und Würmer (Abb. 2), die inzwischen wie Spam-Nachrichten über infizierte und penetrierte „Zombie"-Rechner – meist unter Missbrauch von via DSL breitbandig mit dem Internet verbundenen Privat-PCs – in kürzester Zeit flutartig verbreitet werden. Listen solcher Zombie-Systeme werden von den Entwicklern der Schadensroutinen inzwischen häufig als Verteilernetz Spammern zur Verbreitung angeboten, für sowohl unerwünschte als auch Schaden stiftende Nachrichten.

Bisher haben die in Unternehmen und Behörden eingerichteten technischen „Hürden", wie Virenscanner und Firewalls, dem Ansturm überwiegend Stand gehalten – sofern die Systeme geeignet konfiguriert und systematisch aktualisiert wurden. Dennoch gab es einige erhebliche Schadensfälle: Fast alle bekannt gewordenen spektakulären Schäden wurden jedoch nicht durch Fehler von Scannern oder Firewalls verursacht, sondern von internen oder auch externen Mitarbeitern, die Schaden stiftende Software mit wirksamem Verbreitungsmechanismus über ihre Laptops ins interne Netz einschleusten. Solche „Bypässe" an der Firewall vorbei entsprechen der gefährlichen offenen Hintertüre, die alle Schutzmaßnahmen an der Front Makulatur werden lässt. Die Ursache solcher Sicherheitslücken ist dabei in der Regel nicht in der Technik zu finden – sondern im inadäquaten, leichtsinnigen oder unbedachten Verhalten der IT-Nutzer.

---

1 Dirk Fox, Secorvo Security Consulting GmbH, Karlsruhe; Sven Kaun, Dauth, Kaun & Partner, Karlsruhe.

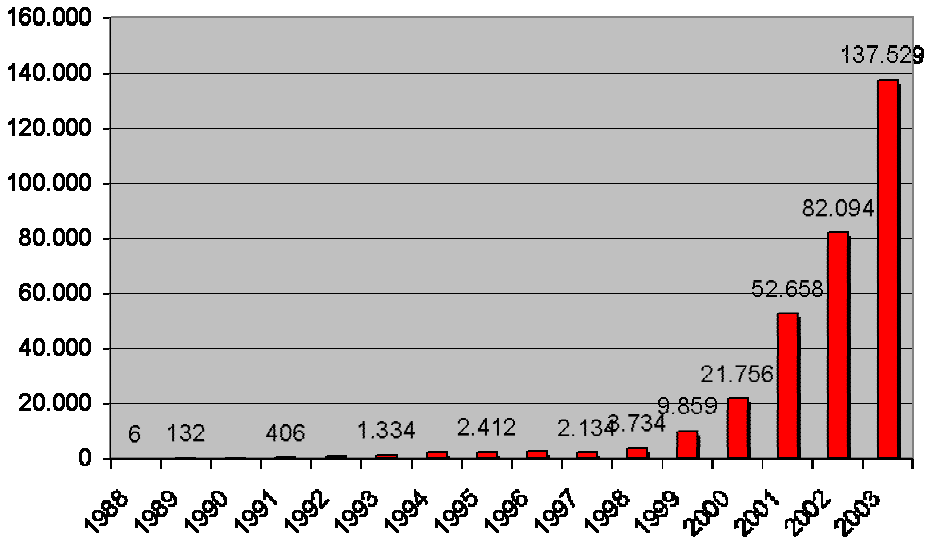

Abb. 1: CERT/CC Vulnerabilities Report (März 2004)

Sollte die Entwicklung der Bedrohungen auch zukünftig nicht an Geschwindigkeit verlieren – wofür es keinerlei Anzeichen gibt: im ersten Halbjahr 2004 wurden pro Woche durchschnittlich 48 neue Sicherheits-Bugs veröffentlicht –, ist absehbar, dass auch die errichteten Schutzwälle eines Tages versagen können: Ein perfider Wurm mit wirksamer Schadroutine, genügend schnell verbreitet, um die Schutzwälle vor der Aktualisierung zu überwinden, könnte erhebliche Schäden anrichten. Eine solche Attacke wird immer wahrscheinlicher, denn mit der Zunahme der Sicherheitslöcher schrumpft zugleich die Zeitspanne zwischen der Veröffentlichung eines Sicherheits-Bugs und der Verfügbarkeit eines passenden Exploits im Internet. Im ersten Halbjahr 2004 ist diese maximale Reaktionszeit auf durchschnittlich 5,8 Tage gesunken – sehr wenig Zeit, um auf Seiten der Hersteller geeignete Software-Patches bereit zu stellen, sie anwenderseitig zu testen und unternehmensweit auszurollen.

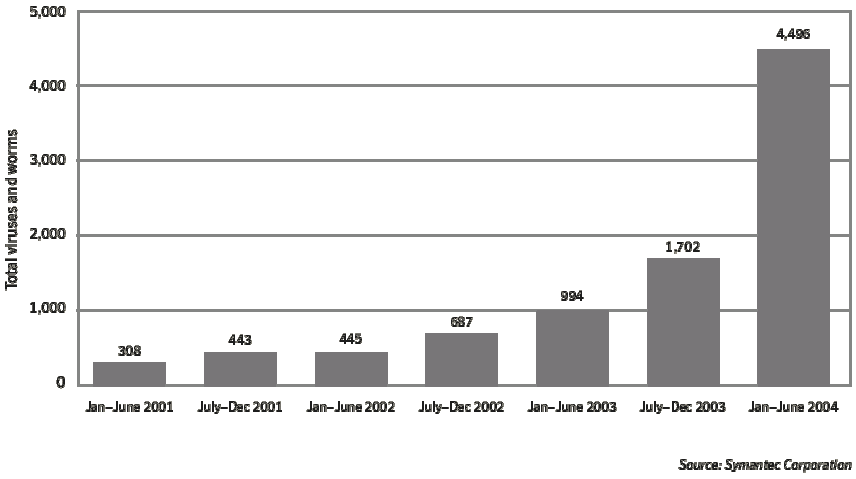

Abb. 2: Symantec Internet Security Thread Report (September 2004)

Auch die zunehmende Mobilität begrenzt die Wirksamkeit zentraler Sicherheitsbarrieren: In wachsendem Umfang werden auch auf mobilen Geräten (Laptops, PDAs, Handys) sensible Unternehmensdaten verarbeitet – und mit den internen Systemen synchronisiert, oder es werden Daten statt über die (kontrollierten) digitalen Kommunikationsverbindungen über einen USB-Speicherstick ausgetauscht. Damit steigt sowohl die Zahl der Verbreitungswege als auch die der Bypässe.

Angesichts dieser Entwicklung werden die Mitarbeiter, lange Zeit als „größter Risikofaktor“ identifiziert, zur letzten Bastion im Schutz der Unternehmensdaten. Aktuelle Umfragen zeigen, dass dies von den meisten Sicherheitsverantwortlichen auch so gesehen wird – gleich nach den Klagen über zu geringe Budgets folgt die mangelhafte Sensibilisierung der Nutzer als größtes Hindernis für eine effektive IT-Sicherheit in deutschen Unternehmen (Abb. 3).

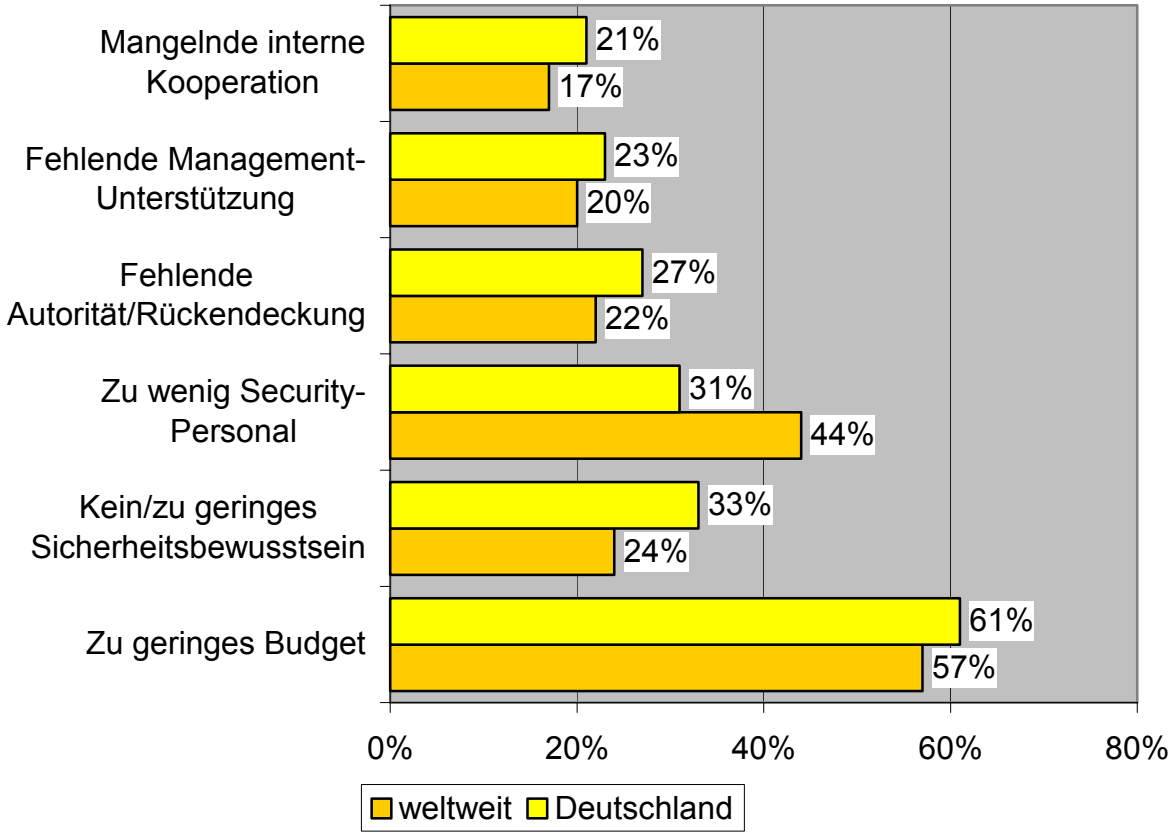

Abb. 3: „Welches sind die größten Hindernisse für eine effektive IT-Sicherheit in Ihrem Unternehmen?“ (The State of Information Security 2004, CIO-Magazin und PWC, September 2004, 8.000 Teilnehmer)

Konsequenter Weise wird in denselben Befragungen die „Verbesserung des Sicherheitsbewusstseins“ als dringendste strategische Maßnahme für 2005 gesehen (Deutschland: 58 % der Befragten).

Viele Unternehmen haben bereits in den vergangenen Jahren intensiv in die Sensibilisierung ihrer Mitarbeiter investiert. Am wirkungsvollsten waren dabei umfassende Awareness-Kampagnen, die darauf zielten, Maßnahmen der Informationssicherheit

aus der ungeliebten Ecke der „Verhinderer“ heraus zu holen und positiv zu besetzen, idealer Weise sogar als Professionalitäts- und Qualitätsmerkmal im Unternehmen zu verankern. Dafür wurde jeweils ein Bündel unterschiedlicher, stark fokussierter und aufeinander abgestimmter Maßnahmen ergriffen, um einen sensibleren Umgang der Mitarbeiter mit Unternehmensdaten zu bewirken.

Wichtig dabei war die Ansprache der Mitarbeiter auf unterschiedlichen Ebenen: neben der sachlich-kognitiven Ebene zur Vermittlung des für die eigene Urteilsfähigkeit erforderlichen Grundwissens und die Schaffung von Verständnis für getroffene Maßnahmen und Regeln, spielte die emotional-affektive Ebene eine zentrale Rolle: durch Bilder, Claims und Aktionszeichen wurde die Informationssicherheit emotional positiv besetzt. In einigen Unternehmen wurde die Kampagne auch um andere Aspekte der Unternehmenssicherheit – Corporate Security, Datenschutz, Arbeitsschutz, Risk Management/Compliance – erweitert und dadurch in ihrer Wirkung verstärkt.

Im Folgenden werden das dabei wiederholt bewährte „Vier-Phasen-Konzept“ vorgestellt und fünf Faktoren beschrieben, die sich bei der Durchführung von Awareness-Kampagnen als erfolgsentscheidend heraus kristallisiert haben.

2 Das Vier-Phasen-Konzept einer Awareness-Kampagne

Für die Durchführung von Security Awareness Kampagenen hat sich die folgende vierteilige Phasenstruktur bewährt (Abb. 4):

- Erste Phase „Aufmerksamkeit gewinnen“: Ziel dieser Phase ist es, die Mitarbeiter über die Durchführung einer Kampagne zu informieren, ihre Aufmerksamkeit zu gewinnen und sie zu einer aktiven Mitwirkung an den einzelnen Maßnahmen der Kampagne zu motivieren.
- Zweite Phase „Wissen vermitteln und Einstellungen verändern“: Diese zweite Phase dient der Vermittlung des für das Verständnis von Sicherheitsmaßnahmen erforderlichen Hintergrundwissens und hat das Ziel, die Einstellungen und damit auch das individuelle Verhalten der Mitarbeiter zu verändern. Es ist der wichtigste und zugleich anspruchsvollste Teil der Kampagne, die „Hauptphase“.
- Dritte Phase „Verstärkung der Wirkung“: In dieser Phase wird eine dauerhafte Veränderung der Einstellung und des Verhaltens der Mitarbeiter angestrebt. Hier sind Maßnahmen erforderlich, die die Thematik fest im Bewusstsein der Mitarbeiter verankern und die in Phase 2 erreichte Sensibilisierung wach halten.
- Vierte Phase „Öffentlichkeitsarbeit“: Diese Phase ist nicht in jedem Unternehmen sinnvoll und abhängig vom Unternehmenszweck. Häufig ist es jedoch hilfreich, die Durchführung der Kampagne in der Außendarstellung – gegenüber den Kunden, den Aktionären, den Geschäftspartnern, den Kreditinstituten – bekannt zu machen. Ziel dieser Phase ist es, ein positives Vertrauens-Image zu vermitteln und so die Erfüllung gesetzlicher Anforderungen an die Risikovorsorge zu dokumentieren oder möglicherweise sogar den Unternehmenswert zu steigern. Die Phase 4 kann mit den anderen Phasen der Kampagne zeitlich überlappen.

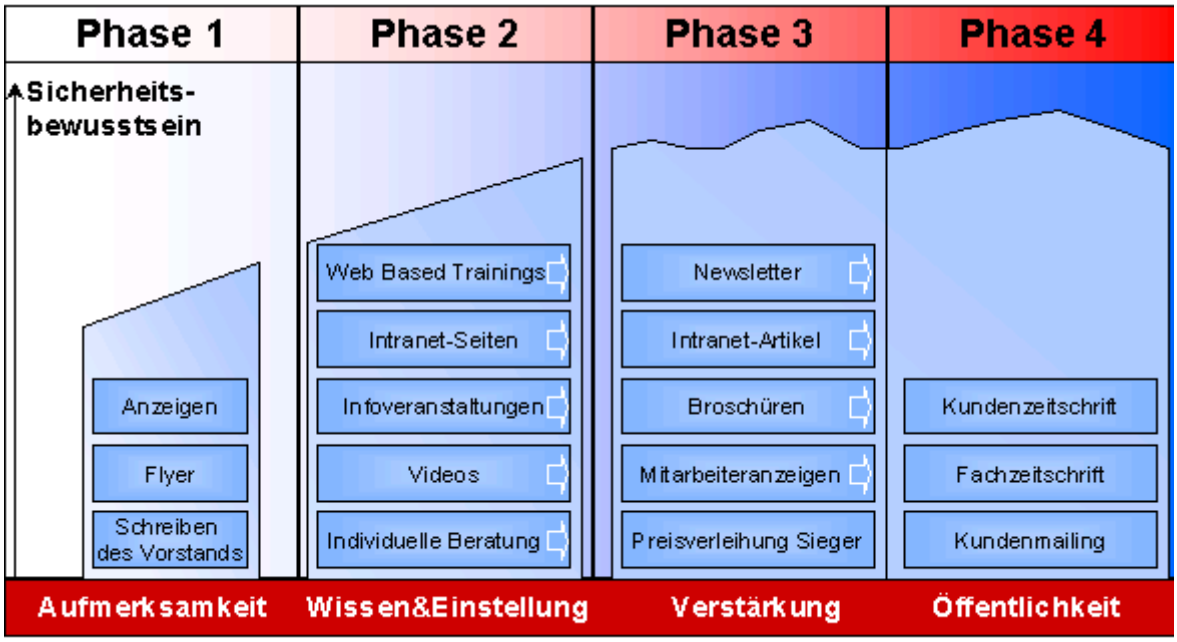

Abb. 4: Vier-Phasen-Konzeption einer Security-Awareness Kampagne

Den vier Phasen der Kampagne vorgeschaltet ist eine Konzeptionsphase, in der die Kampagne im Detail konzipiert und die einzelnen Maßnahmen vorbereitet werden.

3 Erfolgsfaktoren

Als zentrale Erfolgsvoraussetzungen einer Security Awareness Kampagne haben sich vor allem die folgenden fünf Faktoren erwiesen:

- Einbindung des Managements
- „Packende“ Kreativlinie
- Kooperation mit weiteren Unternehmensbereichen
- Modulare Struktur der Hauptphase
- Maßnahmenmix

3.1 Einbindung des Managements

Von besonderer Bedeutung für den Kampagnenerfolg ist eine wirksame Einbindung des Managements in die Durchführung der Kampagne. Sie müssen als unternehmensinterne Multiplikatoren ihren Mitarbeitern die Ziele der Kampagne vermitteln können und vor allem als Vorbild mit gutem Beispiel voran gehen.

Aus diesem Grund sollte vor Beginn der ersten Kampagnenphase eine Veranstaltung zur Information und Einbindung der Führungskräfte durchgeführt werden. Diese Veranstaltung verfolgt vier Ziele:

- Exklusivinformation der Führungskräfte über die Kampagne: Die Führungskräfte werden ca. zwei Wochen vor Beginn der Kampagne umfassend und detailliert über Ziele, Gestaltung und Ausrichtung der Kampagne informiert. Damit werden mögliche Widerstände, die bei der Durchführung ohne ausreichende Information höchst wahrscheinlich wären, im vorhinein vermieden.
- Gewinnung der Führungskräfte für die Kampagnenunterstützung: Von besonderer Bedeutung für den Erfolg der Kampagne ist die aktive Unterstützung der Führungskräfte, z.B. durch Hinweise auf die einzelnen Ereignisse, die Motivation zur und die Unterstützung der Mitarbeiter bei der Teilnahme. Dazu ist es erforderlich, die Führungskräfte nicht nur über den Zweck der Kampagne zu unterrichten, sondern ihnen die Bedeutung des Themas beispielhaft und möglichst anschaulich vor Augen zu führen – sie müssen selbst vom Sinn der Kampagne überzeugt sein, um überzeugen zu können.
- Vermittlung der Rolle und Aufgaben des Managements: Nicht nur während der Kampagne übernehmen die Führungskräfte eine aktiv unterstützende Rolle, sondern sie sind auch hinsichtlich der besonderen Bedeutung eines Informationssicherheit gewährleistenden Verhaltens sowohl in ihrer Motivations- als auch in ihrer Vorbild- und Kontrollfunktion gefordert (Aufklärung der Mitarbeiter, Motivation zur Beschäftigung mit den Themen der Kampagne, Kontrolle der Einhaltung der Regeln).
- Berücksichtigung von Anregungen, Erfahrungen und Wünschen der Führungskräfte: Erfahrungen der teilnehmenden Führungskräfte mit Sicherheitsvorfällen, ihre Kenntnis von existierenden Sicherheitslücken und Vorschläge für die Gestaltung der Sensibilisierungskampagne sollen erfasst und nach Möglichkeit im Verlauf der Kampagne berücksichtigt werden.

Schließlich muss die Informationsveranstaltung die anwesenden Führungskräfte inhaltlich auf Fragen ihrer Mitarbeiter zur Kampagne und zu den in der Kampagne behandelten Kernthemen (s.u.) vorbereiten.

Ergänzend sollte eine Führungskraft als Mentor für die Kampagne gewonnen werden. Der Mentor muss nicht der obersten Führungsebene angehören, sollte jedoch eine möglichst integrative sowie anerkannte Persönlichkeit sein. Sie sollte zudem nach Möglichkeit nicht aus dem IT-Bereich kommen; das verleiht der Mentorenrolle zusätzliche Glaubwürdigkeit und Überzeugungskraft. Im Verlauf der Kampagne sollte dieser Mentor immer wieder „das Wort“ ergreifen – in Form von Interviews, kurzen Statements, Zitaten oder Rundbriefen an die Mitarbeiter.

3.2 „Packende“ Kreativlinie

Die Entwicklung und die durchgängige Verwendung einer einheitlichen Kreativlinie ist sehr wichtig. Sie bildet den Kern der emotional-affektiven Ansprache der Mitarbeiter und zielt auf den „Bauch“. Neben einer klaren Bildsprache mit positiven, in die Unternehmenskultur passenden Assoziationen sollten ein Aktionszeichen und

ein Kampagnen-Claim entwickelt werden, die die Informations- (respektive IT-Sicherheit) positiv belegen und die zentrale Richtung der Kampagne vorgeben.

Kreativlinie, Claim und Aktionszeichen bilden die für die Mitarbeiter erkennbare Klammer um alle Maßnahmen der Kampagne. Sie „verknüpfen“ damit den Aufmerksamkeitswert und die durch einzelne Aktionen erreichte Sensibilisierung und wirken so als Verstärker. Sie erlauben zudem zu einem späteren Zeitpunkt eine thematische Erweiterung der Kampagne (erneute Phase 2), die an die durchgeführten Maßnahmen anknüpft, ohne eine Wiederholung der Aufmerksamkeitsphase (Phase 1) zu erfordern. Diese kommunikative Klammer bestimmt im weiteren Verlauf der Kampagne durchgängig das Erscheinungsbild aller Maßnahmen und Komponenten wie Intranet, Plakate, Flyer und Präsentationen (z. B. im Rahmen von Informationsveranstaltungen). Sie sorgen so für einen hohen Wiedererkennungsgrad.

Bei der Entwicklung von Kreativlinie, Claim und Aktionszeichen muss das Corporate Design des Unternehmens und sollte auch die Bildsprache der Außendarstellung berücksichtigt werden, damit sie in Übereinstimmung mit dem Unternehmensselbstverständnis (Eigenbild) steht. In die Entscheidung über die „richtige“ Kreativlinie sollte nach Möglichkeit auch die Unternehmensleitung eingebunden werden.

3.3 Kooperation mit weiteren Unternehmensbereichen

Aus mehreren Gründen ist eine enge Kooperation mit anderen Unternehmensbereichen schon zu einem frühen Zeitpunkt der Kampagne zu empfehlen. Der wichtigste ist sicherlich, für die Durchführung der Kampagne Unterstützung aus allen betroffenen Bereichen zu gewinnen. Aber auch die Erfahrungen anderer Bereiche sind wertvoll für die Kampagnenkonzeption; deren Berücksichtigung erhöht die Wahrscheinlichkeit einer hohen Wirksamkeit der Kampagne.

Zu den zu berücksichtigenden Unternehmensbereichen zählen vor allem:

- Die Unternehmenskommunikation: Nicht nur ein CI-konformes Erscheinungsbild der Kampagne, sondern auch die Erfahrungen mit unternehmensinternen Kampagnen zu anderen Themen lässt sich viel effizienter und wirksamer in enger Zusammenarbeit mit der Unternehmenskommunikation realisieren. Daher sollte im Koordinationsteam der Kampagne die Unternehmenskommunikation vertreten sein.
- Der Betriebsrat: Eine Security Awareness Kampagne kann in mehreren Punkten die Zuständigkeit des Betriebsrats tangieren, so zum Beispiel bei der Durchführung einer Befragung der Mitarbeiter mit dem Ziel, die Wirksamkeit einzelner Maßnahmen zu evaluieren, oder aber auch bei Weiterbildungsmaßnahmen mit abschließender Zertifizierung. Daher sollte der Betriebsrat über die geplanten Maßnahmen ständig informiert werden; sollten Bedenken gegen einzelne Maßnahmen bestehen, lassen sie sich frühzeitig ausräumen.

- Die Unternehmenssicherheit: Security Awareness Kampagnen werden derzeit in der überwiegenden Zahl der Unternehmen von den für IT-Sicherheit Verantwortlichen initiiert und vorangetrieben. Dennoch umfasst das Thema Informationssicherheit – vor allem auch in der Wahrnehmung und dem Arbeitsalltag der Mitarbeiter – zahlreiche weitere Fragestellungen, die mit Informationstechnik wenig zu tun haben, aber ebenso wichtig sind, wie beispielsweise das Wegschließen sensibler Unterlagen, das Schreddern vertraulicher Dokumente oder der bedachte Umgang mit Betriebsgeheimnissen in öffentlichen Räumen (z.B. bei Telefonaten im Zug oder in Wartesälen).

Bevorzugt sollten diese Unternehmensbereiche bereits an der Konzeption der Kampagne beteiligt werden. Ein solches kooperatives Vorgehen reduziert die Zahl möglicher späterer Reibungspunkte und vergrößert das „kreative Potential“ in der Konzeptionsphase.

3.4· Modulare Struktur der Hauptphase

Die Hauptphase (Phase 2) der Kampagne sollte sich auf wenige zentrale Themen konzentrieren. Es hat sich gezeigt, dass sich durch eine Fokussierung auf eine klar abgegrenzte Fragestellung und Zielsetzung (z.B. Vermittlung der Passwort-Policy) in jeweils einem Modul und Zeitabschnitt der Kampagne eine größere und länger anhaltende Wirkung erzielen lässt als durch die parallele Vermittlung mehrerer Themen und Fragestellungen.

Die Kernthemen der Hauptphase sollten aus den im Unternehmen besonders relevanten, aus Mitarbeiterfehlverhalten resultierenden Sicherheitsmängeln ausgewählt werden. Das in Abschnitt 2 vorgestellte Phasenmodell erlaubt es zudem, zu einem späteren Zeitpunkt mit weiteren Modulen in einer neuen Phasen 2 mit einem veränderten thematischen Fokus zusätzliche Fragestellungen der Informationssicherheit zu vermitteln – orientiert z.B. an aktuellen Ereignissen oder Entwicklungen.

3.5 Maßnahmenmix

Menschen reagieren sehr unterschiedlich auf verschiedene Kommunikationsformen und Medien. Zwar gilt es als erwiesen, dass selbst erarbeitete Lösungen einen höheren Lerneffekt haben als Lernen durch Zuhören oder durch Zuschauen. Bekannt ist aber auch, dass Mitarbeiter über bestehende unternehmensinterne Kommunikationswege (Intranet, Mitarbeiterzeitschrift, Business TV, E-Mails, Rundschreiben etc.) stark unterschiedlich angesprochen und damit verschieden gut erreicht werden.

Es ist daher zu empfehlen, mit einem möglichst breit angelegten Mix unterschiedlicher didaktisch-pädagogischer Maßnahmen zu arbeiten. Zwar sollten die eigenen Erfahrungen des Unternehmens mit der Wirksamkeit einzelner Maßnahmen berücksichtigt werden, denn je nach Unternehmenskultur wirken z.B. Plakate, E-Mails oder Intranet-Informationen sehr unterschiedlich. Dennoch ist es wichtig, zentrale Informationen auf unterschiedliche Weisen zu vermitteln, um möglichst viele

Mitarbeiter zu erreichen. Dazu ist auch eine auf unterschiedliche Zielgruppen im Unternehmen zugeschnittene Aufbereitung der Inhalte wichtig – IT-Administratoren bringen andere Kenntnisse und Voraussetzungen für die Beschäftigung mit dieser Thematik mit als reine IT-Anwender.

4 Literatur

[Fox_03] Fox, Dirk: Security Awareness – Oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit. Datenschutz und Datensicherheit (DuD) 11/2003, S. 676-680.

[RuWN_02] Rudolph, K.; Warshawsky, Gale; Numkin, Louis: Security Awareness. In: Bosworth, S.; Kabay, M.E.: Computer Security Handbook, 4th Edition, Chapter 29 (2002); http://www.nativeintelligence.com/awareness/cshch29kr.PDF

[WiHa_03] Wilson, Mark; Hash, Joan: Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, October 2003.