

Security Awareness

Oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit

Dirk Fox

Schon seit vielen Jahren wird sie immer wieder beklagt und durch Befragungen belegt: die mangelhafte Sensibilität der IT-Nutzer in Unternehmen und Behörden für Belange der Informationssicherheit. Nur wenige Unternehmen haben sich bisher dieses Problems systematisch angenommen. Das scheint sich nun zu ändern. Der Beitrag stellt Ansätze und Methoden zur Benutzersensibilisierung vor und diskutiert die praktischen Aspekte der „Herausforderung Security Awareness“.

Einleitung

Trotz aller Bemühungen und Investitionen der vergangenen Jahre: IT-Sicherheit ist nach wie vor eine tägliche Herausforderung. Nimmt man die dem CERT/CC gemeldeten Vorfälle als Indikator für die quantitative Bedrohungszunahme (Abb. 1), dann hat sich die Zahl der Angriffe seit 1998 jährlich näherungsweise verdoppelt. Das gilt zweifellos auch für die „Dunkelziffer“ aller erfolgreichen Angriffe, die von den Verantwortlichen überhaupt nicht bemerkt werden.

Die schiere quantitative Dimension des Problems nähert sich langsam einer Größenordnung, die ohne aktive Mitwirkung der IT-Nutzer nicht mehr beherrscht werden kann. Hinzu kommt, dass viele technische Schutzmaßnahmen durch Nachlässigkeit, Unwissenheit und oft auch Bequemlichkeit der Nutzer unwirksam werden. Typische Beispiele für Sicherheitslücken dieser Art sind die Versendung und der Empfang ausführbarer Dateien per E-Mail (mit modifiziertem Dateinamen, damit der zentrale

Virens Scanner die Übertragung nicht blockiert), die Installation von Software aus unzuverlässiger Quelle (auch Updates!) und die Nutzung eines ungesicherten privaten Internet-Zugangs mit dem dienstlichen Laptop (ohne Personal Firewall).

Security Awareness rückt daher aus guten Gründen zunehmend in den Fokus der Unternehmenssicherheit. Vielen Verantwortlichen ist bewusst geworden, dass sich das Sicherheitsniveau in ihrem Unternehmen ohne eine Erhöhung des Sicherheitsbewusstseins der Mitarbeiter nicht steigern lässt, denn die meisten Sicherheitsmechanismen und vor allem auch die unvermeidlichen organisatorischen Regelungen erfordern im Kern die positive und aktive Unterstützung aller Mitarbeiter. Die Informationssicherheit hat damit den Menschen „wiederentdeckt“.



Dipl.-Inform.
Dirk Fox

Security Consultant
und Geschäftsführer
der Secorvo Security
Consulting GmbH.
Arbeitsschwerpunkt:
Public Key Infra-

strukturen, Security Awareness, Sicherheit in Netzen.

E-Mail: fox@secorvo.de

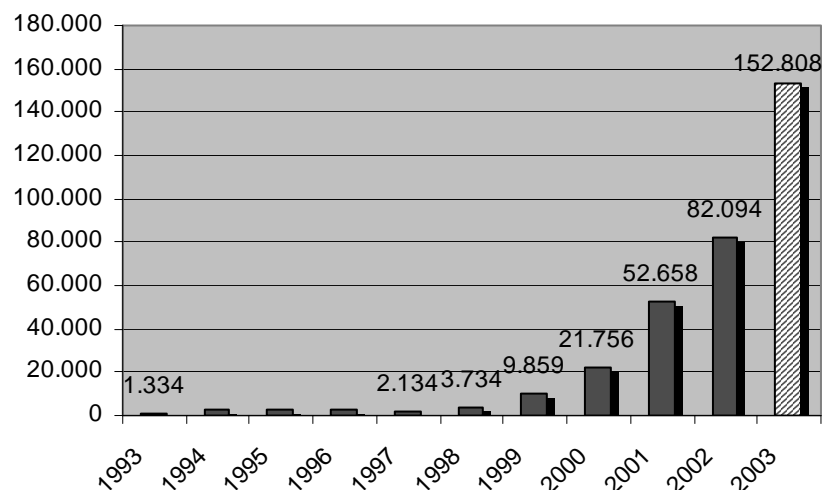


Abb. 1: Gemeldete Sicherheits-Vorfälle beim CERT/CC; 2003: Erwartungswert (http://www.cert.org/stats/cert_stats.html)

1 „Risikofaktor Mensch“

Studien liefern seit vielen Jahren den Beleg, dass Sicherheitsverletzungen der IT-Infrastruktur überwiegend von den eigenen Mitarbeitern verursacht werden. Diese Zahlen mögen einen hohen Fehleranteil haben – einerseits aufgrund der z. T. nur eingeschränkt repräsentativen Auswahl der Befragten, andererseits, weil Angriffe von außen häufig überhaupt nicht bemerkt werden.

Umgekehrt gilt jedoch, dass das Fehlverhalten von Mitarbeitern einen externen Angriff erst ermöglichen kann, wenn beispielsweise sensible Unternehmens- oder Kundendaten unverschlüsselt auf einem Laptop gespeichert werden und dieser entwendet wird, oder aber kritische Informationen ohne Schutz per E-Mail verschickt und von Dritten unberechtigt zur Kenntnis genommen werden.

Ursache des Fehlverhaltens sind in den seltensten Fällen (die es allerdings auch gibt) Vorsatz oder kriminelle Energie der eigenen Mitarbeiter. Die „Regel“ ist Fehlverhalten aufgrund von Unkenntnis oder Missachtung von Sicherheitsbestimmungen, aber auch aus fehlender Übung im Umgang mit etablierten Schutzmechanismen oder einer aus Bequemlichkeit resultierenden Nachlässigkeit.

Die zuletzt genannten Fälle haben eine gemeinsame Hauptursache: eine mangelhaft ausgeprägte Sensibilität der Mitarbeiter für die Bedeutung der Informationssicherheit im eigenen Unternehmen. Darüber sind sich auch die Sicherheitsverantwortlichen einig: Bei einer Befragung von silicon.de von Mai 2002 unter 480 Verantwortlichen für IT-Sicherheit betonten 78 %, das Sicherheitsbewusstsein der Mitarbeiter sei der wichtigste Faktor effektiver IT-Sicherheitsmaßnahmen. Demgegenüber beklagten in der KES/KPMG-Studie im Frühjahr 2002 von 260 befragten Teilnehmern 65 % das fehlende Sicherheitsbewusstsein der Mitarbeiter, und 45 % bezeichneten den Kenntnisstand der IT-Nutzer als „eher schlecht“.

Tatsächlich spricht auch die Verteilung der Investitionen im Bereich IT-Sicherheit eine deutliche Sprache. Eine aktuelle Untersuchung von Ernst & Young belegt, dass wider besseres Wissen in den meisten Unternehmen technische Maßnahmen den Schwerpunkt der Investitionen ausmachen – die „weichen“ Themen der IT-Sicherheit,

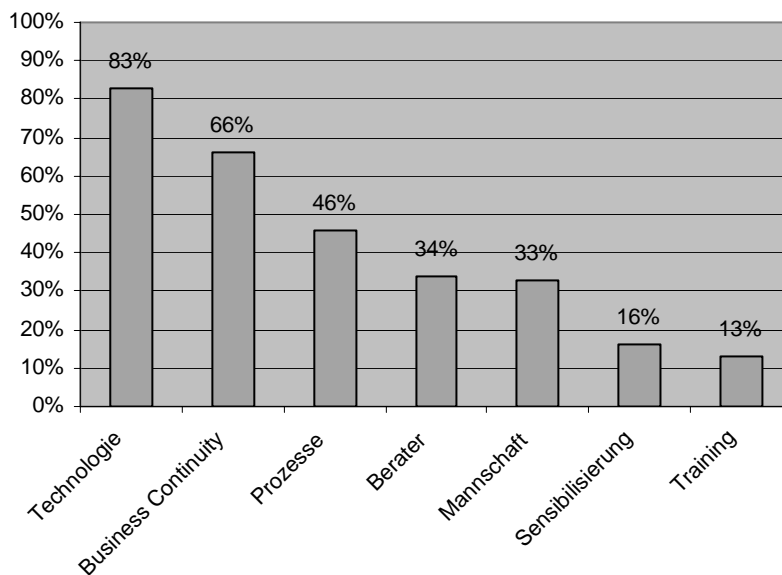


Abb. 2: Investitionen in IT-Sicherheit 2003; Quelle: Ernst & Young (2003)

wie Training und Sensibilisierung, folgen abgeschlagen an letzter Stelle (siehe Abb. 2). Dabei ist die Bedeutung des eigenen, sicherheitssensiblen Verhaltens als Beitrag zum Unternehmenserfolg (und damit zur Sicherung des eigenen Arbeitsplatzes) in den meisten Unternehmen heute sehr unmittelbar. Denn nicht nur der Verlust wichtiger Daten oder der Verfügbarkeit zentraler IT-Systeme kann heute ein Unternehmen schnell in der Existenz bedrohen. Auch das Risiko einer Rufschädigung (z. B. bei einem Datenschutzverstoß), einer hohen Haftung (z. B. bei Verstößen gegen Vertraulichkeitsvereinbarungen) oder einem Verlust von Marktanteilen im Falle einer Ausspähung von z. B. Entwicklungsdaten nimmt mit der wachsenden Bedeutung elektronischer Informationen und Kommunikationssysteme ständig zu.

Einer gesteigerten Sensibilität der Mitarbeiter wirkt allerdings häufig entgegen, dass die zunehmend dramatischen Vorfälle in den Unternehmen aus Angst vor Reputationsverlust sogar intern verschwiegen werden. Damit wird den eigenen Mitarbeitern eine sicherheitstechnisch „heile Welt“ vorgegaukelt, die die Aufmerksamkeit der Mitarbeiter eher einschläfert denn motiviert.

Hinzu kommt, dass Schutzmaßnahmen, die häufig mit hohen Investitionen entwickelt und eingeführt wurden, von den Nutzern überwiegend negativ und störend empfunden werden:

- ◆ als *Arbeitsbehinderung*, da die Nutzung von Sicherheitsmechanismen Arbeitsabläufe verlängert, zusätzliche Passwörter gemerkt werden müssen oder auch Daten nur mittelbar und nicht mehr jederzeit zugänglich sind;
- ◆ als *überzogen*, weil die den Sicherheitsmechanismen konzeptionell zu Grunde liegenden Bedrohungsannahmen als unrealistisch abgetan werden („Bisher ist noch nie etwas passiert“) oder aus Unkenntnis oder Unverständnis Mindestanforderungen z. B. an die Länge von Passwörtern übertrieben erscheinen;
- ◆ als *ungeeignet*, weil die Verantwortung für die Sicherheit der Systeme Dritten, z. B. der IT-Abteilung oder dem Sicherheitsbeauftragten zugewiesen und zugleich die Bedeutung des eigenen Verhaltens unterschätzt wird.

Wie so oft „stinkt“ leider auch hier der „Fisch“ vom Kopf: 50 % der Befragten der KES/KPMG-Studie beklagten die fehlende Unterstützung durch das (Top-) Management. Aber auch eigene Versäumnisse wurden offenbar: Nur bei 51 % der befragten Unternehmen sind die Mitarbeiter mit den IT-Sicherheitsrichtlinien des Unternehmens vertraut (Digital Trust Survey, 12/2002,) – vermutlich obendrein ein optimistischer Wert, denn befragt wurden die Verantwortlichen für IT-Sicherheit (aus 2.100 Unternehmen), nicht aber die Mitarbeiter.

2 Mitarbeiter-sensibilisierung

Die Sensibilisierung der IT-Nutzer für die Belange der Informationssicherheit ist tatsächlich eine größere Herausforderung, als auf den ersten Blick offensichtlich. Denn

- ◆ das Thema Informationssicherheit konkurriert mit einer Vielzahl von Anforderungen „fachfremder“ Art, die ein IT-Nutzer im Rahmen seiner Aufgabenerfüllung beachten soll oder muss;
- ◆ die aktive Unterstützung der Belange der Informationssicherheit setzt nicht nur eine grundlegend positive Haltung zu diesem Thema voraus, sondern erfordert elementares fachliches Verständnis einiger grundlegender Prinzipien;
- ◆ tatsächlich verursachen einzelne Sicherheitsmaßnahmen zusätzlichen Aufwand in bestehenden Arbeitsabläufen und strapazieren damit die positive Grundeinstellung der IT-Nutzer.

Zentrale Voraussetzung für eine auch langfristig wirksame Sensibilisierung der IT-Nutzer ist daher eine solide Konzeption der zu treffenden Maßnahmen, die geeignet ist, die folgenden (Teil-) Ziele zu erreichen:

- ◆ die Gewinnung der *Aufmerksamkeit* für das Thema „IT-Sicherheit“ (z. B. durch ein entsprechendes Rundschreiben des Vorstands, internes „Marketing“ etc.);
- ◆ die *Gewinnung des Interesses* der Mitarbeiter für Maßnahmen der IT-Sicherheit;
- ◆ die *Vermittlung von Grundwissen*, um ein elementares Verständnis für die Bedeutung und Ausgestaltung von Maßnahmen der IT-Sicherheit zu ermöglichen;
- ◆ die *Vermittlung von Praxiswissen*, das bei Sicherheitsvorfällen den Mitarbeitern situationsadäquate Reaktionen erlaubt;
- ◆ die *Aufrechterhaltung des Interesses* am Thema durch regelmäßige und aktuelle Informationen und Nachrichten über einen längeren Zeitraum.

Für die Erfüllung dieser Voraussetzungen gibt es zahlreiche Möglichkeiten und Hilfsmittel. Allerdings scheitert die Umsetzung leicht an internen Hindernissen. So ist häufig das Verhältnis zwischen IT-Abteilung und IT-Nutzern keineswegs entspannt: Die zahlreichen Geschichten über den „DAU“, den „dümmsten anzunehmenden User“, lassen erahnen, wie weit viele IT-Abteilungen von einer Dienstleistungshaltung entfernt sind, die die Ursache von Fehlern nicht zuerst in der Dummheit

des Anwenders, sondern in der mangelhaften Vermittlung und Anleitung suchen.

Hinzu kommt, dass Maßnahmen und Konzepte zur erfolgreichen Sensibilisierung nicht allein technische Kenntnisse erfordern – sie stellen hohe Anforderungen an die didaktische, pädagogische und kommunikative Kompetenz der für die Durchführung Verantwortlichen, Qualifikationen also, die meist nicht zur Kernkompetenz der IT-Abteilung zählen und daher Unterstützung aus anderen Unternehmensbereichen oder durch externe Partner nahe legen.

3 Awareness-Kampagnen

Ein probates Mittel, um Mitarbeiter für die Informationssicherheit im Unternehmen zu sensibilisieren, ist die Durchführung von Awareness-Kampagnen. Das Ziel einer solchen Kampagne ist ehrgeizig, denn es soll schließlich kein kurzfristiger „Strohfeuerereffekt“, sondern eine langfristige Verhaltensänderung von Mitarbeitern erreicht werden. Inhaltlicher Kern einer solchen Kampagne ist üblicherweise das Regelwerk der IT Security Policy des Unternehmens oder der Behörde, das konkrete Verhaltensanforderungen und -anweisungen formuliert.

3.1 Die Phasen der Kampagne

Üblicherweise wird eine Awareness-Kampagne auf einen längeren Zeitraum von bis zu mehreren Jahren angelegt. Dabei lassen sich prinzipiell vier Phasen unterscheiden (Abb. 3):

- ◆ Die **„Aufmerksamkeitsphase“**: Ziel dieser Phase ist es, die Aufmerksamkeit der Mitarbeiter zu gewinnen und sie zu einer aktiven Mitwirkung an den einzelnen „Bausteinen“ der Awareness-Kampagne zu motivieren.

Diese Phase beginnt mit der Erarbeitung des Gesamtkonzepts der Awareness-Kampagne. Anschließend werden gemeinsam mit der für die Unternehmenskommunikation zuständigen Abteilung ein Kampagnen-Logo und ein Claim als „Brand“ entwickelt, die sich anschließend als „roter Faden“ durch alle Teile der Kampagne ziehen und einen hohen Wiedererkennungswert darstellen.

Von besonderer Bedeutung gleich in dieser ersten Phase ist die Einbindung des Managements z. B. durch ein Rundschreiben des Vorstands an alle Mitarbeiter.

- ◆ Die Phase **„Wissen vermitteln und Einstellungen verändern“**: Die zweite Phase dient der Vermittlung des für das Verständnis von Sicherheitsmaßnahmen erforderlichen Wissens und hat das Ziel, Einstellungen der IT-Nutzer (und damit auch das individuelle Verhalten) zu verändern. Es ist der wichtigste und zugleich anspruchsvollste Schritt der Kampagne.

In dieser Phase werden nicht nur die zentralen Inhalte (Informationen und Appelle, Regelwerk der IT Security Policy) der Kampagne vermittelt, sondern das pädagogisch ehrgeizige Ziel einer nachhaltigen Einstellungs- und Verhaltensänderung in sicherheitsrelevanten Belangen soll erreicht werden. Hilfreich sind daher eindrucksvolle Darstellungen, die haften bleiben und die IT-Nutzer in relevanten Fällen an das „richtige“ Verhalten erinnern.

Eine sehr wirkungsvolle Methode zur Gewinnung und Aufrechterhaltung des

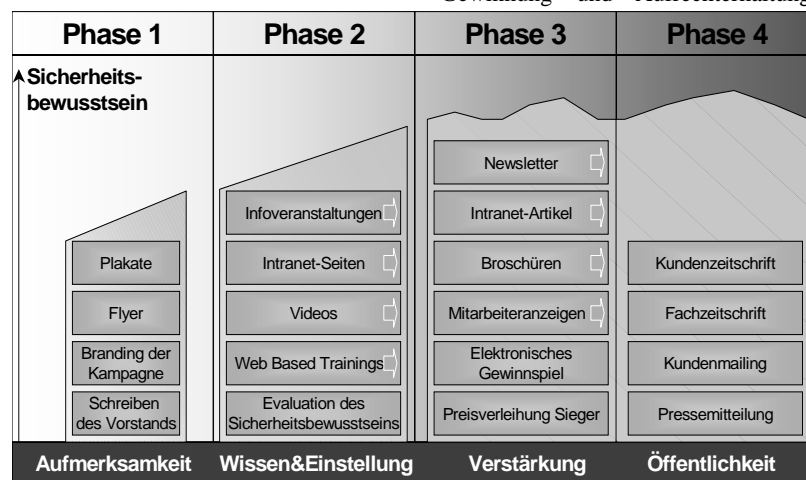


Abb. 3: Die vier Phasen einer Security Awareness-Kampagne

Interesses der Mitarbeiter ist die Vermittlung der Möglichkeiten zum Schutz des privaten PC beispielsweise vor Viren und Angriffen aus dem Internet. Da Spam, Würmer, Trojaner, 0190-Dialer und die sichere Übertragung sensibler Daten (Kreditkartennummer, Kontoverbindung, PIN/TAN) die Mitarbeiter als Privatpersonen betreffen, kann die Sensibilisierung für die Risiken der privaten Nutzung des Internet die Entwicklung einer höheren Sensibilität für Sicherheitsbelange des Unternehmens erheblich befördern.

- ♦ Die Phase der „**Verstärkung**“: In dieser Phase wird eine dauerhafte Veränderung der Einstellung und des Verhaltens angestrebt. Hier sind Maßnahmen empfehlenswert, die die Thematik fest im Bewusstsein der Mitarbeiter verankern und wach halten.

Durch eine kontinuierliche Auseinandersetzung mit dem Thema wird sichergestellt, dass die Mitarbeiter ein starkes Bewusstsein für Informationssicherheit entwickeln und sich zukünftig in sicherheitsrelevanten Situationen professionell verhalten.

Als Bausteine dieser Phase, die zugleich den Höhepunkt der Kampagne darstellt und die größte „Maßnahmendichte“ umfasst, kommen regelmäßige Newsletter, die das Thema aktuell halten, die Verteilung von Broschüren zu ausgewählten Themen der IT-Sicherheit (z. B. Informationen über aktuelle Maßnahmen), Gewinnspiele und interessant gestaltete Beiträge in der Mitarbeiterzeitung in Betracht. Eine weitere Maßnahme können intensive Trainings für Mitarbeiter in besonders sensiblen Bereichen wie der Entwicklungs- und der Personalabteilung oder dem Vorstandsbereich sein.

- ♦ Die Phase „**Öffentlichkeit**“: Nach der Devise „Tun Sie Gutes und reden Sie darüber“ kann es wünschenswert sein, die Durchführung der Kampagne in der Außendarstellung des Unternehmens und der Öffentlichkeit bekannt zu machen. Ziel dieser Phase ist es, den Kunden ein positives Vertrauens-Image zu vermitteln möglicherweise damit sogar den Unternehmenswert zu steigern.

Die konkreten Maßnahmen können dabei von Berichten in Kundenzeitschriften über Kunden-Mailings und Pressemitteilungen bis hin zu Anzeigen oder Aufsätzen in Publikumszeitschriften reichen.

3.2 Ergebnismessung

Um schließlich die tatsächliche Wirkung und die Änderung von Einstellungen messbar zu machen, sollte gleich zu Beginn und nach Abschluss der zweiten Phase der Kampagne eine repräsentative, anonyme und Web-basierte Befragung der Mitarbeiter durchgeführt werden, aus deren Ergebnissen eine zumindest qualitative Bewertung des bestehenden Niveaus des Sicherheitsbewusstseins und der erreichten Veränderung abgeleitet werden können.

Diese Befragung sollte zur Überprüfung der Nachhaltigkeit der Mitarbeitersensibilisierung zu einem späteren Zeitpunkt der Kampagne oder auch in definierten Zeitabständen nach Abschluss der Kampagne (beispielsweise im Rahmen von regelmäßigen Audits) wiederholt werden.

4 Lernen mit WBTs

Ein zentraler Baustein bei der Vermittlung des erforderlichen Grundwissens ist die Nutzung von Web basierten Trainings (WBT, E-Learning-Komponenten). Gegenüber reinen Präsenztrainings erlauben E-Learning-Einheiten nicht nur ein selbstgesteuerteres Lernen und verringern die Kosten je Lerner, sondern ermöglichen auch eine Orientierung an unterschiedlichen Wissensständen, die Berücksichtigung verschiedener Lerntempi und Lerntypen.

entierten Präsenztrainings zum Konzept des sogenannten „Blended Learnings“ verknüpft: Das Web Based Training dient dabei der Vermittlung von Grundwissen zur Angleichung des Wissensstands der Teilnehmer vor Beginn des Präsenztrainings sowie einer effizienten Nachbereitung des Gelernten.

Wichtig bei der Gestaltung eines Web Based Trainings zur Informationssicherheit sind vor allem drei Aspekte:

- ♦ Die *Adressierung unterschiedlicher Zielgruppen*: Nicht jede Lernergruppe wird von denselben Inhalten angesprochen, und nicht jede Person im Unternehmen benötigt dieselben Informationen. So werden IT-Administratoren deutlich weitergehendere Informationen von dem Training erwarten als Mitarbeiter des Empfangs; umgekehrt kann es sein, dass ein Lerner zur persönlichen Überzeugung umfassendere Informationen sucht als ein anderer, dem ein grobes Übersichtsverständnis genügt.
- ♦ Die *Motivation der Nutzer*: Die Gestaltung von inhaltlichen Teilen des Web Based Trainings, die den Mitarbeiter auch als privaten Nutzer von IT-Systemen ansprechen („Wie schütze ich mich privat?“), Testfragen, die mit der Ausstellung eines Zertifikats verknüpft sein können oder auch die Teilnahme an einem internen Preisausschreiben können motivierende Begleitmaßnahmen sein.

Der Mensch behält von dem, was er

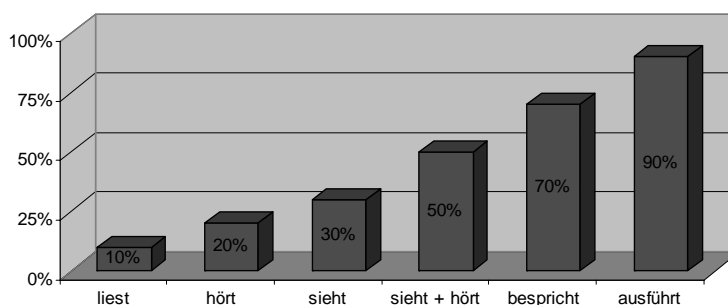


Abb. 4: Nachhaltigkeit von Lernmethoden (aus: W. Kowalczyk, K. Ottich, „Schülern auf die Sprünge helfen“, 1995)

Lernmethodisch lassen sich Präsenztrainings allerdings nicht vollständig durch Web Based Trainings ersetzen. Denn der Lernerfolg betreuter Übungen („Lernen durch Tun“) wird von multimedialen Web Based Trainings (mit Bild und Ton) nicht erreicht. Daher werden heute üblicherweise Web-basierte Lerneinheiten mit übungsori-

- ♦ Die *Möglichkeit zur flexiblen Nutzung*: Das WBT muss unter unterschiedlichen Arbeitsbedingungen (Großraumbüro, unterschiedlich leistungsfähige Recherausstattung z. B. mit/ohne Audio, „mobile“ Umgebung) genutzt werden können und auch Unterbrechungen vertragen (Lernstandspeicherung).

5 Awareness-Maßnahmen

Um die Aufmerksamkeit der Nutzer über einen längeren Zeitraum aufrecht zu erhalten und so eine nachhaltige Wirkung zu erzielen, muss eine Awareness-Kampagne insbesondere kreative und ansprechende Einzelelemente enthalten. Diese Elemente sollten zur Erzielung eines hohen Wiedererkennungswerts unter einem einheitlichen gestalterischen Auftritt zusammengefasst werden (Motto, Logo, grafische Gestaltung).

Dabei sollten neben einem Web Based Training zur Wissensvermittlung, Einheiten des Blended Learnings für ausgewählte Zielgruppen und Plakate etc. weitere effektvolle „Tools“ zum Einsatz kommen. Dies können z. B. sein:

- ◆ Videos zur Sensibilisierung, die Angriffe auf IT-Systeme und ihre Wirkungen eindrucksvoll demonstrieren
- ◆ internes Preisausschreiben, das eine inhaltliche Auseinandersetzung der Teilnehmer mit Themen der Informationssicherheit „erzwingt“ und mit attraktiven Preisen zur Teilnahme motiviert
- ◆ ansprechende „Give-Aways“, die Mitarbeiter als „Mahner“ täglich an Belange der IT-Sicherheit erinnern (z. B. Post-Its mit der Aufschrift „Bitte hier Passwort notieren und unter Tastatur kleben“, Kalender mit Cartoons, ...)

- ◆ privat nutzbare Hilfsmittel zur IT-Sicherheit (z. B. CDs mit Sicherheits-Freeware-Tools für den Home-PC)
- ◆ Newsletter mit interessanten Hintergrundinformationen, Geschichten, aktuellen Nachrichten
- ◆ Intranet-Portal mit Materialien (Richtlinien, Gesetzestexte, weiterführende Dokumente wie White Paper o. ä.) und aktuellen Informationen
- ◆ Web-basierte Bedienungstrainings für neue Sicherheitslösungen

Diese Maßnahmen müssen in der Gesamtkampagne inhaltlich eng verzahnt werden und so aufeinander abgestimmt sein, dass das Interesse der Mitarbeiter nicht abreißt und über die Kampagne hinaus wach gehalten wird. Zudem sollten die Maßnahmen verknüpft werden mit der internen Weiterbildung (Durchführung von Prüfungen und Ausstellung von qualifizierenden Zertifikaten), dem Führungskräfte-Training sowie den Prüfanforderungen interner Sicherheits- und Datenschutz-Audits.

Fazit

Angesichts der wachsenden Bedeutung von Information in Unternehmen aller Branchen nehmen Maßnahmen zu deren Schutz zunehmend einen wichtigen Platz in der allgemeinen Risikovorsorge ein. Dies wird nicht zuletzt in den Regelungen des Aktengesetzes (AktG), des Gesetzes zur Kontrolle

und Transparenz im Unternehmen (KonTraG), von denen zahlreiche Bestimmungen analog auf GmbHs übertragbar sind, und der neuen Eigenkapitalvereinbarung des Basler Ausschusses für Bankenaufsicht („Basel II“) deutlich.

Ein wirkungsvoller Informationsschutz steht und fällt jedoch mit der aktiven Unterstützung durch alle Mitarbeiter des Unternehmens. Daher haben auch internationale Standards der IT-Sicherheit wie BS 7799 (ISO 17799) die Förderung des Sicherheitsbewusstseins der Mitarbeiter als Forderung aufgenommen.

Häufig aber werden Sicherheitsmaßnahmen von IT-Nutzern in erster Linie als Arbeitsbehinderung betrachtet, wird die eigene Verantwortung nicht wahrgenommen oder werden vernünftige Risikoannahmen der Verantwortlichen als realitätsfern abgetan – und damit Bedrohungen der Informationssicherheit durch das Verhalten von Mitarbeitern mitverursacht.

Durch geeignete Security Awareness-Kampagnen können sowohl das erforderliche Grundwissen vermittelt, die Sensibilität der Mitarbeiter für Informationssicherheit erhöht als auch Einstellungen und Verhaltensweisen nachhaltig verändert werden.

Zahlreiche Unternehmen haben inzwischen Awareness-Kampagnen gestartet oder planen deren Durchführung.¹

Das pädagogisch anspruchsvolle Ziel einer Verhaltensänderung lässt sich jedoch nicht durch Stroheffereffekte erreichen, sondern nur durch ein strukturiertes, auf Dauer angelegtes Maßnahmenkonzept, das IT-Sicherheit als ein Kriterium der internen Qualitätsbewertung (ggf. sogar einer Leistungsbewertung auf Leitungsebene) etabliert und immer wieder die Aufmerksamkeit der Mitarbeiter gewinnen kann.

Literatur

[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>

¹ Das zeigte u. a. die große Resonanz auf das diesjährige „Security Awareness Symposium“ am 24.-25.06.2003 (<http://www.security-awareness-symposium.de>).



Abb. 5: Beispiel eines WBTs zur Informationssicherheit (Firma digital spirit ag, Berlin, <http://www.digital-spirit.de>)