Nr. 5, Oktober 2008

<kes>

Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

BSI Forum

offizielles Organ des BSI

Bundesamt für Sicherheit in der Informationstechnik

<kes>/Microsoft-Studie 2008:

Lagebericht zur Informations-Sicherheit (2)

S. 55

Virtualisierung:

Stolperfallen und wie man sie vermeidet

S. 14

SYSTEMS 2008 mit IT-SecurityArea

Vorschau auf Produkte und Aussteller S. 26

SecuMedia

Wollen, Wissen – und was dann?

Security-Awareness benötigt Handlungsspielraum

Sicherheitsbewusstsein und -wissen sind in Awareness-Projekten lediglich Mittel zum Zweck. Der Motivation und Befähigung muss auch die Gelegenheit zur Umsetzung des Gelernten folgen – das kann ein ganzes Unternehmen aufrütteln, es aber auch im Sinne der Unternehmensentwicklung voranbringen.

Von Michael Helisch, München

Worauf kommt es bei Vorhaben zur Security-Awareness an? Ist es die Unterstützung durch das Top-Management? Ist es die pfiffige Kampagne, die versteht, Mitarbeiter auf die (Sicherheits-)Reise mitzunehmen? Oder die Art der Wissensvermittlung und Motivation? Irgendwie klingt das alles wichtig und richtig – ist es auch, reicht aber trotzdem nicht! Analysiert man den methodischen Aufbau von Awareness-Kampagnen, dann sind zwei Bausteine nahezu immer enthalten: Wollen und Wissen. Aber was kommt, wenn diese Ziele erreicht wurden?

Doch zunächst zurück zum Anfang: Mit zum Teil enormem Kommunikations- und Marketingeinsatz wird (zu Recht) versucht, den Mitarbeitern die fürs Unternehmen besonders relevanten Sicherheitsaspekte schmackhaft zu machen. Aufmerksamkeit schaffen und Interesse wecken, führt – so die Annahme – zur richtigen Einstellung der Belegschaft in Sachen Sicherheit. Und mit der richtigen Einstellung ist es dann nur noch ein kleiner Schritt bis zum richtigen (sicherheitskonformem) Verhalten. Spätestens dann kommt die Wissensvermittlung ins Spiel und wird Bestandteil von Awareness: Denn schließlich sollen die Mitarbeiter ja nicht irgendwas tun, sondern das Richtige (im Sinne der definierten Sicherheitsrichtlinien und -prozesse). So weit, so gut!

Danach wird es aber erst richtig spannend: Geht es nun doch an die praktische Umsetzung dessen, was man bis dahin gesehen, gehört, gelernt und vielleicht auch schon mal spielerisch ausprobiert hat! Die von Sicherheit frisch begeisterten Kollegen Müller und Mayer wissen nun, was zu tun ist, und wollen sicherheitskonform handeln. Jetzt kommt es darauf an, ob sie es auch können – und zwar sowohl im Sinne von „Zeit finden" als auch im Sinne von „verwirklichen dürfen": Wer vor lauter Arbeit nicht weiß, wo ihm der Kopf steht, macht sich kaum Gedanken um die Sicherheit! Und wo solche Gedanken aufkeimen, brauchen sie immer noch einen fruchtbaren Boden, um wachsen und erblühen zu können.

Wie es nicht sein soll, ist schnell erzählt: Nehmen wir Frau Mayer – eine Mitarbeiterin, die sich nunmehr bewusst ist, dass die Informationen, mit denen sie Tag für Tag arbeitet, wirksam geschützt werden müssen. Jüngst kam ihr die Idee, man könnte doch die Bürotüren, die bislang gänzlich ohne Schlösser mehr oder minder nur dem Schallschutz dienten, mit selbigen versehen lassen: Denn wieso ständig darauf achten, den PC beim Rausgehen zu sperren, vertrauliche Dokumente, an denen man nach dem Mittagessen ohnehin noch weiterarbeiten muss, sorgsam wegzuschließen und so weiter – alles ginge doch viel einfacher und sicherer, wenn man schlicht das Büro abschließen könnte! „Ja schon, Frau Mayer", meinte dazu ihr Chef, „aber was das kostet, alle Büros nachträglich mit Systemschlössern auszustatten?! Den Kollegen vom Controlling sehe ich schon jetzt die Hände überm Kopf zusammenschlagen. Könn'se vergessen!"

Man ahnt, wie schnell die Errungenschaften einer ebenso erfolgreichen wie teuren Awareness-Kampagne durch derlei Unterstützung „genullt" werden. So motiviert Frau Mayer den Weg zu ihrem Chef antrat, so desillusioniert begibt sie sich auf den Rückweg in ihr immer noch unverschlossenes Büro: „Sicherheit ist wichtig, zeigen Sie Initiative!" war eine zentrale Botschaft des Awareness-Projekts, erinnert sie sich – „Von wegen!"

Das Leben danach

Sicherheit lebt von und mit praktikablen Lösungen. Was nützt es, wenn ein Mitarbeiter sicherheitskonform handeln will und weiß, was zu tun ist, aber die technisch-organisatorische Infrastruktur ein solches Handeln anschließend nicht adäquat unterstützt?! Sicherheitssensibilisierte Mitarbeiter werden Fragen und Vorschläge äußern wie im Beispiel, wenn die Awareness-Kampagne erfolgreich war – auch teure, unliebsame und möglicherweise sogar unpraktikable. Gut, wenn dann der Ansprechpartner überzeugender reagiert als Frau Mayers Chef!

Ist Sicherheit wirklich wichtig? Für den nachhaltigen Erfolg von Awareness-Aktivitäten ist die Unterstützung aller Management-Ebenen unerlässlich! Das Top-Management muss hier mit gutem Beispiel vorangehen. Aber: Sicherheit ist selbst mit „Management-Backing" bisweilen lediglich ein weiteres von vielen „Topics of Corporate Relevance". Was, so die berechtigte Frage des Mitarbeiters, ist denn nun wirklich wichtig? Weniger ist da manchmal mehr!

„Leben" wir das, was wir als wichtig definieren? Unternehmens-Werte sind Ausdruck der Unternehmens-Kultur. In vielerlei unternehmensinternen Medien werden sie ausführlich beschrieben und kommuniziert. Was, wenn diese Werte zwar ausführlich beschrieben sind, es aber an der konsequenten Umsetzung im beruflichen Alltag mangelt? Wenn schon zentrale Werte von der Unternehmensführung nicht glaubhaft vorgelebt werden, warum sollte dies beim vermeintlich nachrangigen Wert „Sicherheit" der Fall sein? Auch vor diesem Hintergrund besteht die akute Gefahr, dass Awareness-Aktivitäten nicht den Effekt erzielen, den sie eigentlich erzielen könnten. „Konsequenz" heißt hier das Zauberwort!

Gesamtkunstwerk

Passen Sicherheitsanforderungen und Unternehmenskultur zusammen? Gegenseitige Wertschätzung und Vertrauen sind Unternehmenswerte, die man auf zahlreichen Webpräsenzen findet. Das Vertrauen, das man als Mitarbeiter des Unternehmens seinen Kolleginnen und Kollegen quasi „per se" entgegenbringt, ist leider auch ein immer wieder gern verwendeter Ansatzpunkt für Social Engineering. Da werden dem Angerufenen ein paar vermeintliche (weil mittels Google leicht recherchierbare) Interna zugeworfen und schon nimmt der Angerufene an, der Anrufer sei „einer von uns". In den meisten Fällen wird daraufhin bereitwillig Auskunft gegeben.

Arglistiges Täuschen trifft in solchen Szenarien nicht selten auf blindes Vertrauen. Doch wie damit umgehen? Die kritische und konsequente Auseinandersetzung mit den verschiedenen Facetten der Unternehmenskultur ist eine Möglichkeit. Dies sollte allerdings nicht erst im Verlauf der Umsetzung von Awareness-Aktivitäten erfolgen, sondern vielmehr deren Basis sein.

Allerdings begibt sich der Sicherheitsverantwortliche dabei auf „dünnes Eis", denn er verlässt nicht nur seinen qua Rolle ausgeübten Zuständigkeitsbereich, sondern rüttelt an den Grundfesten des Unternehmens, indem er zu dieser Auseinandersetzung aufruft. Kann und will er das? Birgt die kritische Auseinandersetzung auf der anderen Seite aber auch die Chance, die Unternehmenskultur den veränderten Gegebenheiten anzupassen und das

Security-Awareness aus werbepsychologischer Sicht

Sicherheit konkurriert mit einer Vielzahl weiterer unternehmensinterner Themen. Aus Sicht der Mitarbeiter wird Sicherheit aber nur dann wichtiger als andere Themen wahrgenommen, wenn man sie *systematisch vermarktet:* Dies bedeutet, sich der grundlegenden Erkenntnisse der allgemeinen Psychologie (Wahrnehmung, Lernen, Persönlichkeit), der Sozialpsychologie (psychische Prozesse aufgrund sozialer Interaktion), der Soziologie (soziale Schicht, Normen, Gruppendruck) sowie der Biologie und Medizin (Aktivierung und Reizverarbeitung) zu bedienen, um die Sicherheit wie gewünscht zu platzieren.

Vergleicht man die bekanntesten Modelle der Werbewirkung miteinander, so lassen sich verschiedene Stufen psychologischer Zielgrößen ableiten. Meist geht es zunächst darum, eine bestimmte Sinneswirkung zu erzielen (Aufmerksamkeit, Interesse), als letzte Stufe wird fast durchgängig ein bestimmtes Verhalten genannt – im klassischen Werbekontext der Kauf als solcher. Zwischen diesen beiden Polen erfolgt je nach Modell eine unterschiedlich starke und differenzierte kognitive und emotionale Auseinandersetzung mit dem jeweiligen „Objekt der Begierde".

Sicherheitsbezogene Kommunikation erfordert einen Spagat zwischen fachlich-inhaltlicher Richtigkeit und ansprechenden, leicht verständlichen Inhalten. Da allein der Empfänger, bewusst oder unbewusst entscheidet, ob und welche Wirkung das Gesendete hat, ist er der Souverän der Nachricht. Deshalb ist es unerlässlich, die Interessenslage der Zielgruppe(n) genau zu kennen, um die dazu passenden Botschaften zu senden.

Der Empfänger macht die Nachricht

Um aus Zuschauern aktive Mitstreiter zu machen, darf auch die konstruktive Auseinandersetzung mit dem Thema kein Tabu sein. Zudem gilt es, den Mitarbeiter zu aktivem Handeln zu bewegen und wo immer möglich die persönliche Kommunikation mit ihm zu suchen – dass dies ein zeitintensives Unterfangen ist, liegt auf der Hand. Das Investment lohnt aber durchaus, denn schließlich wird neben der Sache auch der Sicherheitsverantwortliche selbst vermarktet.

Kommunikation ist Ausdruck der Unternehmenskultur und erfolgt nach bestimmten impliziten und expliziten Regeln. Sie darf hinsichtlich Form und Inhalt aber ruhig auch einmal ungewohntes Terrain beschreiten, um die gewünschte Aufmerksamkeit zu schaffen. Dabei ist jedoch Fingerspitzengefühl gefragt, damit sich der gewünschte Effekt nicht ins Gegenteil verkehrt.

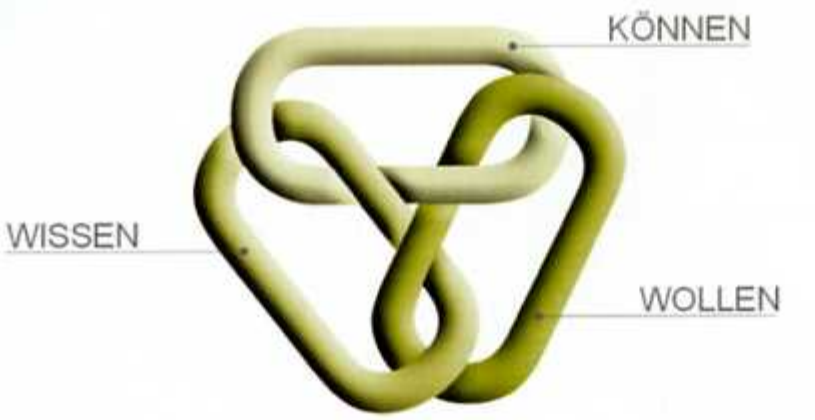
Für Awareness gibt es zudem nur selten eine einzige Zielgruppe: Bei größeren, besonders bei international agierenden Unternehmen kann schnell das halbe oder ganze Dutzend voll werden. Die für die einzelnen Zielgruppen beschlossenen Awareness-Maßnahmen wollen dann aber dennoch so koordiniert sein, dass sich alles zu einem schlüssigen Gesamtbild zusammenfügt. Damit Systematik, Konsistenz und die definierten Kommunikationsziele erreicht werden, bedarf es einer zentralen Persönlichkeit, die ein stets wachsames Auge auf das Gesamtbild wie auch „Time and Budget" der Awareness-Aktivitäten hat.

Kontext-Sicht und Erfolgskontrolle

Awareness-Kommunikation ist jedoch nur die halbe Miete: Sie muss in den Gesamtkontext „Mensch im Unternehmen" eingebettet sein. Dieser setzt auf den Ergebnissen einer Analyse der Unternehmens- und daraus abgeleitet der Sicherheitskultur auf. Zu diesem Gesamtrahmen gehören wiederkehrende Schulungen (in Person oder übers Web), die mit dokumentierbarem Erfolg von allen Mitarbeitern zu durchlaufen sind. Ob das gewünschte Ziel erreicht wurde, lässt sich dann mittels verschiedener Befragungs- und Beobachtungsmethoden beantworten (Audits, Social-Engineering-Assessments, Analyse von Vorfällen etc.). Die gewonnenen Erkenntnisse geben wiederum Input für weitere Maßnahmen. Ganzheitliche Awareness-Arbeit ist damit stetige und langfristig angelegte Kommunikation, Change-Management und in manchen Fällen ein stückweit Organisationsentwicklung.

Wirkungsstufe	Kriterium der Marketingwirkung
Ausgangslage	Individuelle Prädisposition
Wirkungsstufe 1	Aufmerksamkeit und Wahrnehmung
Wirkungsstufe 2	Verstehen der Werbebotschaft
Wirkungsstufe 3	Einstellung, Image, Kaufabsicht
Wirkungsstufe 4	Handlung (z. B. Kauf)
Wirkungsstufe 5	Handlungswiederholung

Systematisches Vermarkten – auch von Sicherheit – erfolgt über verschiedene Stufen hinweg



Wollen, Wissen und Können sind in Awareness-Projekten untrennbar miteinander verwoben.

Unternehmen so sicherer und stärker zu machen? Diese Fragen mit „ja" zu beantworten und entsprechend zu handeln, dazu bedarf es neben Mut zur Initiative auch der richtigen Mitstreiter im eigenen Hause sowie Konsequenz und Ausdauer im Handeln.

Fazit

Interesse für Sicherheit zu wecken, dieses Interesse in Engagement und Verantwortungsbewusstsein zu verwandeln sowie Wissen zielgruppengerecht zu vermitteln, das sind wichtige und richtige Aspekte von Security-Awareness. Die Rahmenbedingungen zu schaffen, damit derart sensibilisierte Mitarbeiter ihr Wissen und Wollen in der täglichen Arbeit auch tatsächlich umsetzen können, ist eine weitere, wenn nicht die größte Herausforderung erfolgreicher Awareness-Arbeit.

Hierbei geht es um mehr als nur um Sicherheit: Es geht darum, hinter die Kulissen menschlichen Handelns im Unternehmen zu schauen, Unternehmensprozesse und -kultur zu hinterfragen. Dass der für Sicherheit Verantwortliche dabei seinen originären Verantwortungsbereich verlassen muss und sich auf mitunter ungewohntes Terrain begibt, liegt auf der Hand. Dabei entsprechend konsequent voranzuschreiten, erfordert Mut und Ausdauer. Dieser Mut führt letzten Endes aber zu den besseren Ergebnissen nicht nur in Bezug auf das Thema Sicherheit, sondern auch für das ganze Unternehmen – Security-Awareness wird damit gleichzeitig ein Stück weit Unternehmensentwicklung. ■

Dipl.-Kaufmann Michael Helisch ist Inhaber von Hecom Security Awareness Consulting.