olé

Der Security-Newsletter
hrsg. von known_sense

6 Juni 2007

Awareness + Unternehmenskultur + Elektronische Kampfkunst

askit

Sicherheitskultur
– ein strategischer Wettbewerbsvorteil
von Marcus Beyer

askit – awareness security kit
Weltweit erstes qualitatives Analyse-, Coaching- und Kreationstool für Corporate Security Identity

My Security Tools
Neuer Awareness-Koffer sensibilisiert Entscheider eines globalen Spezialchemikalienherstellers

Zweite tiefenpsychologische Sicherheitsstudie Ende 2007

*Malware als »Bausatz« **VirusBrickMaster** s.a. S. 3*

Innovative Tools werben für Awareness bei Chemikalienhersteller

Sensibilisierte IT-Entscheider: Kampagne für Informationssicherheit hat nun höchste Priorität

Am Anfang war das Virusquartett. Thomas Dallmann, Information Security Manager bei einem globalen Spezialchemikalienhersteller, der dort seit Anfang 2006 den Aufbau einer Abteilung Information Security gestaltet, kannte das known_sense-Awareness-Kartenspiel von Kollegen und aus den Medien. Für ein Treffen der IT-Leitungsebene seines Unternehmens im Mai 2007 in Puerto Rico hatte der Security Manager zunächst zwei Dinge im Sinn, als er bei der Kölner Kommunikationsagentur anklopfte: Erstens wollte er sich einige Dutzend Exemplare der internationalen Version des known_sense-Virusquartetts sichern, um es als Giveaway auf der Karibikinsel an Kollegen und Vorgesetzte zu verteilen. Zweitens die Beauftragung zur Gestaltung eines Plakats zum Thema Information Security, um beim internen Plakatwettbewerb die Fahne für seine Verantwortungsbereich hoch zu halten – sprich: für den Start einer internationalen konzernweiten Awareness-Kampagne ab Ende 2007 zu werben.

Dann kam alles ganz anders. Aus dem einen Poster wurden gleich drei. Das Virusquartett, das es in der englischen Printversion zum Zeitpunkt der Anfrage noch gar nicht gab, wurde kurzerhand gemeinsam mit known_sense im Branding beider Unternehmen unter dem Titel »Computer Beast« neu produziert. Und obwohl man insgesamt nur etwa drei Wochen Zeit für Konzept und Produktion der Sensibilisierungstools hatte, mit denen der Sicherheitsbeauftragte sein Management überzeugen wollte, entstanden in und trotz dieser Kürze weitere Giveaways zum Thema, denen man aufgrund des innovativen Kommunikationsansatzes durchaus einen gewissen Pilotcharakter hinsichtlich modern ausgerichteter Awareness-Kampagnen einräumen muss.

Die Anforderungen

Doch der Reihe nach. Nachdem im Unternehmen zunächst die Top-Themen der Information Security identifiziert wurden,

- Passwörter bzw. Authentifizierung mithilfe neuer Tools (Passwort-Reduktion),
- Klassifizierung von Dokumenten und
- Malware und deren Abwehr (Defense: Strategien, Tools und Personen),

sollten die geplanten Tools vor allem hohes Involvement und Impactstärke kommunizieren. Auch sollten alle Mitarbeiter unabhängig von Standort, Nationalität und damit verbundenem kulturellen Background und Muttersprache angesprochen werden können.

Objekte für die paradoxe Mitarbeiter-Intervention: ***My Password Pad, My Password Pencil, Password Bracket***

Auch alles drin: Von klassischen Postern übers Virusquartett und-Bausätzen bis zu den Objekten für die paradoxe Intervention: ***Your Information Security Tools****, der Entscheiderkoffer, produziert von known_sense*

Die Kreation

Bei der Ideenfindung kam innerhalb der Agentur »askit« (Security Awareness Kit) zum Einsatz, ein Analyse-, Coaching- und Kreationstool, das known_sense u.a. mit den Psychologen und Marktforschern der 2006 ➔

Awareness-Poster aus der Dose

produzierten tiefenpsychologischen Eigenstudie »Entsicherung am Arbeitsplatz – die geheime Logik der IT Security in Unternehmen« entwickelt hatte. Aufgrund der o.g. Ausgangssituation, zu dem durchaus auch die Bereitschaft der Konzernspitze gehörte, das Thema Awareness stärker in den Fokus des Unternehmens zu rücken, entschied man sich für ein spielerisches wie paradoxes Vorgehen.

»Spielerisch« bedeutet, dass die Mitarbeiter via Information Security die »Erlaubnis« erhalten, die sachliche Aufmerksamkeit zugunsten eines experimentellen Vorgehens einschränken zu dürfen und sich so dem Thema auch tatsächlich ganzheitlichen mit allen Sinnen – auch unbewusst und nicht nur kognitiv – öffnen sollten. »Paradox« bedeutet, dass beim Rezipienten via klassischer paradoxer Intervention zunächst Irritation ausgelöst werden sollte, die anschließend durch sachliche Richtigstellung relativiert wird. Der Mitarbeiter erkennt hierdurch aus sich heraus, dass eine »Schieflage« vorliegt und bemüht sich eigenverantwortlich um Korrektur, eine Wirkung, die durch Zustimmung einer sachlich richtigen Aussage, z.B. auf einem Poster – etwa mit dem Slogan »Information Security ist wichtig« - bei weitem nicht erzielt werden könnte.

»Die nachhaltige Wirkung des paradoxen Passworthalters hatte ich bereits innerhalb meines persönlichen Arbeitsumfelds anhand eines Dummies testen können. Dort fragte man stets auch nach, ob es nicht wieder neue Awareness-Objekte von known_sense geben würde,« sagt Thomas Dallmann. Und weiter: »Und da ich selber gerne spiele, weiß ich auch um die enormen Effekt der Wissensvermittlung bei guten Spielen.« So stand für den Security Manager fest, dass er neben den gesetzten klassischen Medien – wie etwa dem Poster – in jedem Fall auch die eher »schrägen«, verspielten und paradox anmutenden Giveaways, für die die known_sense bekannt ist, einsetzen wollte.

»Es war mir wichtig, dass das Thema Information Security über die Tools eine einhundertprozentige Aufmerksamkeit erhält und sich die Adressaten tatsächlich damit beschäftigen,« fasst Thomas Dallmann seine Ansprüche zusammen.

Die Tools

So entstand die Edition »VirusBrickMaster« mit circa 80 Bausteinen einer bekannten Spielzeugmarke in einer thematisch stimmig gestalteten wie attraktiven Metalldose. Mithilfe von »VirusBrickMaster« werden die Mitarbeiter ausgefordert, den letzten Virus, den Sie von Ihrem Rechner entfernt haben, zu visualisieren, indem sie ihn mithilfe der Bausteine »nachbauen«. Eine Art Bauanleitung präsentierte auf vier Seiten bereits fer-→

»Build the last computer virus you removed from your PC, with the bricks inside«. ***VirusBrickMaster*** *mit ca. 80 Bausteinen*

tige Beispiele für »visualisierte Viren« und fordert auf, Fotos persönlicher Viren-Bauwerke via Intranet-Upload unternehmensintern zu veröffentlichen.

Für die Entscheider der ersten Ebene wurde zusätzlich eine Art »Chefkoffer« unter dem Titel »Your Information Security Tools« produziert und konfektioniert. Der transparente Koffer enthielt:

- eine Metalldose (DIN-A4) mit Kofferlabel und (innenliegend) 3 Plakate zu 3 Top-Security-Themen, jeweils eines zu jedem der 3 Themen
- ein Virusquartett »Computer Beast« (englisch) im gemeinsamen Kunden-Agentur-Branding
- ein Konzepthalter mit Gravur »Password Brakket« mit einer »Password Card«, auf dem der User aufgefordert wird, sein Passwort zu dokumentieren – selbstverständlich inklusive der sachlichen Richtigstellung dieser Paradoxie
- ein Block »My Password Pad« zum Aufschreiben von Passwörtern
- ein Kugelschreiber mit Gravur »My Password Pencil«
- eine (limitierte) Edition »VirusBrickMaster«, nummeriert und vom Security Manager eigenhändig signiert.

Die Wirkung

Die Tools lösten noch während der Veranstaltung aufgrund der z.T. paradoxen Logik Verwunderung, aber auch eine intensiver Beschäftigung und eine hohes Maß an Interaktion aus – ganz im Sinne der Anforderung. Eines der Plakate erhielt den ersten Preis beim internen Wettbewerb und das Thema Security Awareness den Segen des Managements, indem ihm nun innerhalb der Information Security Projekte höchste Priorität eingeräumt wird.

Damit haben sich Thomas Dallmanns hoher Einsatz und seine weite Reise gelohnt – in Kürze wir er gemeinsam mit known_sense ein Kampagnenkonzept für eine internationale Awareness-Kampagne an allen Standorten des Unternehmens ausarbeiten, bei dem erneut »askit« und – nach Überarbeitung – auch ein Teil der für Puerto Rico generierten Tools zum Zuge kommen werden. ■

WÖLFE
& GEISSEN
Der Rheinische Security Stammtisch

Corporate Security
& Unternehmenskultur

21.8.2007 18:30 Uhr
Köln/Wein R. Hoffmann
Anmeldung: sense@known-sense.de

WÖLFE
& GEISSEN
Der Rheinische Security Stammtisch

Sicherheitskultur – ein strategischer Wettbewerbsvorteil

von Marcus Beyer – Awareness-Programme sowie eine aktiv gelebte Sicherheitskultur können Unternehmen als Grundlage für einen Wettbewerbs- und Know-how-Vorsprung gegenüber den Mitbewerbern dienen. Die Investition in die Mitarbeiter schützt Unternehmenswerte.

Wird berücksichtigt, dass in 80 Prozent aller Sicherheitsvorfälle der Mensch und nur in 20 Prozent die Technik versagt hat, kann man schnell ein ungenutztes Sicherheitspotenzial bei den Mitarbeitern feststellen. Um Informationssicherheit in einem Unternehmen zu etablieren, werden viele organisatorische Massnahmen ergriff en. Unternehmen betreiben dabei oft eine physische »Sicherheitsaufrüstung«. Sie schotten sich mit allen ihnen zur Verfügung stehenden Sicherheitswerkzeugen ab. Sie reglementieren den Mitarbeitern den Netzzugang und sprechen bei Nicht-Einhaltung von gesetzten Regeln schnell Mahnungen oder gar Kündigungen aus.

Direkte, persönliche Ansprache

Die effizienteste und eigentlich einfachste Massnahme, die der direkten, persönlichen Ansprache, erfolgt mit niedriger Priorität und kommt dementsprechend viel zu kurz. Dies bedeutet eben nicht unbedingt, dass eine verabschiedete Vorgabe, wie sich ein Mitarbeiter zu verhalten hat, jeder Mitarbeiter kennt und für seine tägliche Arbeit verinnerlicht hat.

Trotz des mittlerweile in Managementkreisen salonfähig gewordenen Themas »Informationssicherheit und Security Awareness im Unternehmen« wird in den Unternehmen oft nur das Allernötigste eingeführt. Selten, dass man von einer ganzheitlichen Lösung auch nur im Ansatz reden kann. Dies schaffen nur Ausnahmebetriebe, die es aber durchaus gibt.

Vielen Grossunternehmen gelingt es daher heutzutage kaum noch, den »menschlichen Faktor« im Arbeitsalltag zu integrieren. Sie werden aber keine Sicherheitskultur etablieren können, wenn auch in Zukunft eine entmenschlichte Unternehmenskultur herrscht.

Tiefenpsychologen beschreiben deshalb gar schon ein Horrorszenario: Mitarbeiter, die ganz isoliert und seelisch vollkommen deformiert in einem komplett überwachten und sicherheitstechnisch abgeriegelten Unternehmen sitzen. Gerade durch die technische und organisatorische Beschränkung sucht sich der Mitarbeiter unbewusst Schlupflöcher, um diesem starren und eingenden Martyrium zu entfliehen. Er entsichert hierbei ständig und aus sich heraus.

Image der Sicherheit fördern

Auch das Image der IT beziehungsweise der IT-Sicherheitsabteilung in Unternehmen ist oft nicht optimal. Es herrscht ein gespaltenes Verhältnis zur IT-Abteilung. Einerseits hilft sie durch ihre administrative Präsenz, die Arbeitsverfassung des Einzelnen im gewünschten Rahmen zu halten. Andererseits wird sie von den Mitarbeitern als Exekutive des Systemzwanges im Unternehmen erlebt. In der Regel wird ihr misstrauisch bis ablehnend begegnet. Es fehlt einfach an genügend positiver, aktiver und ehrlicher Kommunikation. Für die Etablierung einer »lebendigen Sicherheitskultur« ist dies aber ein wichtiger Faktor. Gut geplante und durchgeführte Awareness-Programme in Unternehmen lösen in den meisten Fällen auch das »Imageproblem« der IT-Security-Abteilung. Denn dadurch bekommt IT- und Informationssicherheit ein Gesicht und präsentiert in positiver Art und Weise die dazugehörigen Protagonisten. Mitarbeiter von Unternehmen müssen wissen – hier wird nichts verboten, hier wird geschützt – der Mitarbeiter selbst und die Werte des Unternehmens.

Schutz statt Verbote

Dies belegt auch in Ansätzen die Studie »Entsicherung am Arbeitsplatz« von known_sense und Partnern, u.a. dem Autor dieses Beitrags. Diese Studie zeigt deutlich auf, dass hundertprozentige Sicherheit vom Menschen gar nicht auszuhalten ist. Es gilt also, gezielt die Sicherheitskultur in allen Facetten im Unternehmen zu analysieren, um danach individuelle Massnahmen aufzusetzen. Lebendige Awareness-Kampagnen, die eher im Unbewussten wirken, sind effektiv und zielführend. Dadurch wird mehr erreicht als mit offenen Drohungen oder endlos wirkenden IT-Schulungen.

Der Aufbau einer Informationssicherheitskultur ist dann erfolgreich, wenn die Führungskräfte im Unternehmen den Umgang mit sensiblen Daten und der IT gewissenhaft vorleben. Diese Vorbildfunktion ist ein entscheidender Punkt im Aufbau und in der Pflege der Informationssicherheit. Den Führungsstab frühzeitig mit einzubeziehen, entscheidet über den Erfolg jeder Awareness-Massnahme und deren Umsetzung im Unternehmen. Dabei ist allerdings auch darauf zu achten, dass die Umsetzung des Awareness-Programms keine reine IT-Aufgabe ist und bleibt. Die Sicherheitskultur muss abteilungsübergreifend gedacht und geführt werden.

Bisher werden Awareness-Massnahmen klassisch »von oben« gesteuert. »Wissen« wird hierbei oft einfach nur durch ein Quiz oder stichprobenartige Interviews abgefragt. Doch damit ist die Sicherheitskultur➔

eines Unternehmens noch nicht ausreichend analysiert.

Reale Projekte und Werkzeuge

Hier zeigt die Praxis, dass geeignete Werkzeuge in Unternehmen bisher noch nicht weit verbreitet sind, um den Ist- und Soll-Zustand der Sicherheitskultur im Unternehmen zu bestimmen. Das bestätigen auch Risk Manager beziehungsweise Sicherheitsverantwortliche für »Legal Compliance«: »Wir machen in unserem Unternehmen viele Awareness-Massnahmen und Schulungen. Nur können wir leider nicht wirklich nachweisen, ob diese auch ihre Wirkung zeigen.« Gegenüber der Geschäftsleitung beziehungsweise dem Verwaltungsrat müssen aber messbare Ergebnisse als Grundlage geschaffen werden, um die Wirksamkeit ihrer Awareness-Massnahmen zu bestätigen. Und das kontinuierlich.

Mit solchen Werkzeugen lässt sich eindeutig analysieren, wo ein Unternehmen seine Awareness-Ambitionen ansetzen muss, und welche Massnahmen auch wirklich greifen. Massnahmen, die sogar bei den Mitarbeitern nachhaltig wirken. Nicht nur die »Wissensabfrage« muss beleuchtet werden, sondern auch Faktoren wie die Loyalität der Mitarbeiter, deren Motivation und die Sicht auf das interne Wertesystem.

Awareness als Wettbewerbsvorteil

Fragt man Unternehmen, die bereits erfolgreich Security-Awareness-Kampagnen durchführen, nach dem Warum, gibt es meist zwei klare Antworten. Erstens: Wir wollen, sollen und müssen unsere Mitarbeiter mit den Sicherheitsrichtlinien vertraut machen. Zweitens: Dadurch erreichen wir sehr schnell einen Wettbewerbsvorteil gegenüber den Mitbewerbern.

Security Awareness als strategische Grösse im alltäglichen Wettkampf um Marktbesetzung und Kunden – diese These ist nicht mal weit her geholt. Je weniger sensible Informationen das Unternehmen verlassen, um so eher hat man die Chance, auf dem Markt mit einem Produkt oder einer Dienstleistung ein »First Mover« (mit einer guten Reputation) zu sein. Wirtschaftskriminalität rangiert in Studien und Statistiken über die Ängste von Unternehmenslenkern auf einem der oberen Plätze. Aber auch die klassische Sicht auf die »Business Continuity« ist hier relevant. Die Räder stehen eben nicht still, nur weil ein Mitarbeiter aus Unwissenheit einen Virus oder Trojaner ins Unternehmensnetz gesaugt hat. Denn er weiss ja nach einer erfolgreichen Security-Awareness-Kampagne, was er tut – sollte er zumindest.

»Incident Response« gegenüber den Sicherheitsverantwortlichen im Unternehmen ist hier das Schlagwort – selbst gesteuert und durchgeführt durch sensibilisierte Mitarbeiter. Ist der Blick geschärft, wird mit allem Fremden kritischer umgegangen. Setzt der gesunde Menschenverstand rechtzeitig ein, kann von einer Kulturveränderung im Unternehmen gesprochen werden.

Organisationsanpassungen

Die Sensibilisierung von Mitarbeitern und die damit verbundenen Massnahmen oder die Security-Awareness-Kampagne als solche führen dabei oftmals nicht nur zu einer Kulturveränderung, sondern fordern auch Organisationsanpassungen im Unternehmen. Wenn Mitarbeiter während des Awareness-Programms positiv »provoziert« und zum Handeln angeregt werden, bekommen IT- und Organisationseinheiten viel zu tun, denn hier wird Awareness pure Realität. Auf jede Massnahme muss auch eine Umsetzung erfolgen. Wenn Mitarbeiter sensibilisiert werden, dann werden sie auch aktiv! Was hilft es, Mitarbeitern zu erklären, dass Dokumente wegzuschliessen sind (Clean-Desk-Ansatz), wenn der Schlüssel für den Aktenschrank fehlt, oder vertrauliche Dokumente geschreddert werden müssen, in der Abteilung aber nirgends ein Schredder zur Benutzung steht? Security Awareness ist also Umsetzung pur.

Informationssicherheit braucht daher eine offene und ehrliche Kommunikation – ohne den erhobenen Zeigefinger. Security Awareness ist eben nicht nur ein Wissens-, sondern auch ein Wettbewerbsvorsprung. ■

Marcus Beyer
ist Architect Security Awareness
bei Ispin AG in Bassersdorf.
Er leitet Projekte für
Sicherheitskultur und
Mitarbeitersensibilisierung.
Marcus.beyer@ispin.ch

askit – awareenss security kit: neues known_sense-Tool

»Wirkungsanalysen Corporate Security Identity und Emotional Security Communication & Awareness«

Mit askit (security awareness kit) hat known_sense das erste qualitative Analyse-, Coaching- und Kreationstool, konzipiert, das Unternehmenssicherheit und deren Risiken im Kontext aller relevanten Faktoren behandelt – auch derer, die auf den ersten Blick nicht unmittelbar zum Security-Umfeld gehören. Auf der Grundlage von askit analysieren Experten aus den Feldern Unternehmens- bzw. Managementberatung, IT/ Information Security, Kommunikation/ Journalismus, Psychologie/Coaching, Kreation/Design Ihre Corporate Security Identity im Kontext der in ihrem Unternehmen herrschenden und für Ihre Branchen typischen Unternehmenskultur, um auf dieser Basis Learnings für die Optimierung von Prozessen Ihrer Unternehmenssicherheit und Kommunikationskonzepte für Ihre laufend wie geplanten Security Awareness-Kampagnen abzuleiten.

askit ist ein »lernendes« Tool, d.h. es wird auf der Grundlage aktueller known_sense-Forschungs-Projekte, z.B. die aktuelle Studie, oder Kunden-Projekte (etwa. Awareness-Kampagnen) regelmäßig weiterentwickelt. Bisher existieren die beiden askit-Module ACC (Analyse – Consulting – Coaching) und KIK (Kreation – Implementierung – Kommunikation)

Analyse nach askit

- Umfassende Analyse des unternehmensspezifischen Umgangs mit Informationssicherheit sowie des Verhältnisses von Sicherheitskultur und Unternehmenskultur
- Qualitative Wirkungsanalyse von Policies, von bestehenden Security-Produkt- und Awareness-Kampagnen
- Identifikation von Zielgruppen- und Standort-Differenzierungen

Mithilfe der morphologischen Psychologie, die an der Universität Köln entwikkelt worden ist, analysieren erfahrene Diplom-Psychologen sowie Markt- und Medienforscher die unbewussten seelischen Einflussfaktoren und Sinnzusammenhänge. Vorgenommen werden die Analysen, die zielgruppen-, branchen-, kultur- und standortspezifische Unterschiede differenzieren, auf Basis von Beobachtungen, Auswertungen der Materialien, die vom Unternehmen zur Verfügung gestellt werden, sowie mithilfe von Tiefeninterviews.

Diese werden im Rahmen eines schriftlichen Berichtsbandes fixiert und z.T. auch visualisiert, damit Sie sich ein Bild Ihrer Securitykultur machen können. Die analytische Ebene wird zudem durch Empfehlungen von weiteren Experten ergänzt, die Ihnen erfolgsversprechende Maßnahmen vorschlagen. Bei allen folgenden Prozessen bilden diese Expertisen die strategischen Grundlagen für das weitere Vorgehen von der Beratung über die Kreation bis hin zur Erfolgskontrolle.

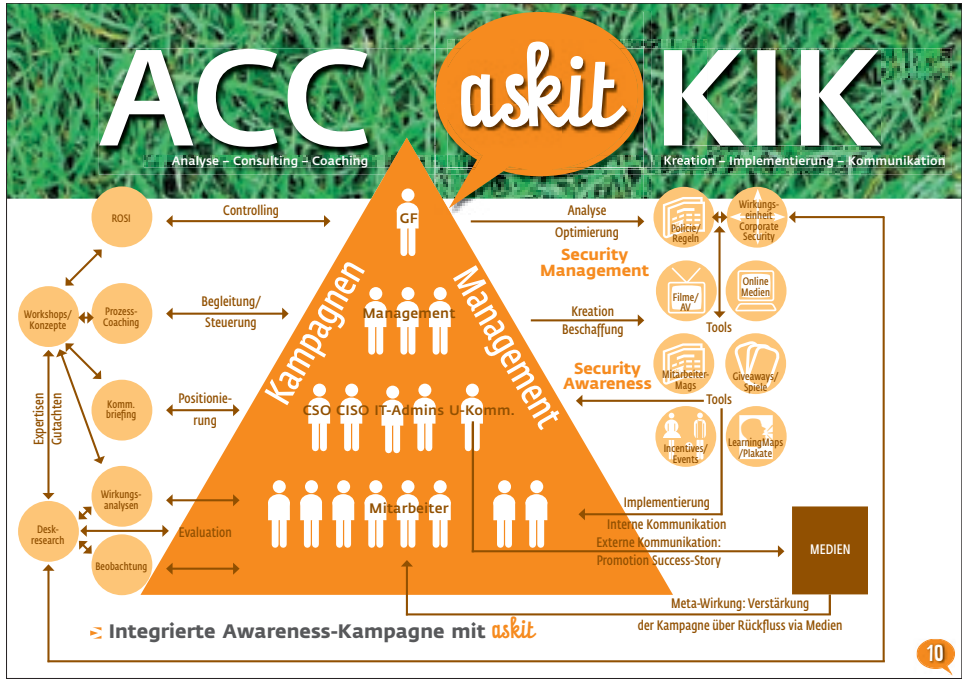
In tiefenpsychologischen Interviews können die verdeckten Motive, die das Verhalten des Einzelnen im Umgang mit Informationssicherheit beeinflussen, erfasst und in einen psycho-logischen und relevanten Kontext gebracht werden. Auf Basis dieser grundsätzlichen Ergebnisse können dann zielgenaue und konkrete Empfehlungen zu innerbetrieblichen Maßnahmen zur Verbesserung der Informationssicherheit formuliert werden.

Das psychologische Tiefeninterview nach askit verbindet Bedeutungstiefe mit Erkenntnispragmatik. In zweistündigen Einzel- oder Gruppenexplorationen decken die known_sense-Experten die oft unbewussten seelischen Wirksamkeiten➔

und Einflussfaktoren auf, die das Verhalten aller von der Corporate Security betroffenen Personen bestimmen. Dabei eröffnen sich neue und oft überraschende Einblicke. Der zugrunde liegende Leitfaden ist ein lernender Leitfaden, d.h. in Tiefeninterviews überraschend auftretende Aspekte können innerhalb nachfolgender Interviews berücksichtigt werden. Damit liefert eine askit-Analyse intensive und wissenschaftlich abgesicherte Ergebnisse auf Basis von kleinen, aber aussagefähigen Stichproben. Hierbei reicht auch eine verhältnismäßig kleine Stichprobe aus, da bei psychologischen Tiefeninterviews die wirksamen Motivkomplexe und Einflussfaktoren in jedem Einzelinterview vollständig repräsentiert sind. Theoretisch ist die Psycho-Logik einer Wirkungseinheit sogar bereits in einem (1!) idealen Interview erfassbar – mithin interessant und auch wirtschaftlich realisierbar für Kleinstunternehmen und KMUs.

Consulting

- Beratung bei der Entwicklung einer unternehmensförderlichen Security-Umgebung
- Beratung bei Kreation, Auswahl und Beschaffung von Awareness-Tools/-Medien



Der Ansatz von askit sieht den Umgang mit unternehmensbezogenen Sicherheitsmaßnahmen davon geprägt, wie der einzelne das Unternehmen als Ganzes, und seine Stellung innerhalb dieser „Arbeitsfamilie" erlebt. Hierbei ist die Frage zu stellen, welcher konkreter Sinn z.B im entsichernden Verhalten von Mitarbeitern zum Ausdruck. Technische Lösungen – auch innovative – behandeln stets nur die Symptome von Sicherheitslecks, nicht aber die wirklichen Ursachen. Da im Gegensatz hierzu der Mensch nicht einfach mit einer neuen Software ausgestattet oder eliminiert werden kann, wenn er nicht »funktioniert«, muss es mithin zu einer »Behandlung« kommen. Diese kann über sinnvoll aufeinander abgestimmte Sensibilisierungsmaßnahmen oder beispielsweise über Coachings bzw. Workshops in das Unternehmen implementiert werden.

Coaching und Controlling

- Entwicklung eines Kommunikationsbriefings für CSOs und beteiligte Berater/Agenturen
- Prozess-Coaching für IT-Administratoren/CSOs bei der Entwicklung von →

Awareness-Maßnahmen und -Tools sowie Training, Schulungen, etc.
> Prozess-Coaching, u.,a. zur Maßnahmen-Erfolgsevaluation (ROSI = Return Of Security Invest).

Beim speziell für Sicherheitsbeauftragte und Entscheider konzipierten Prozess-Coaching werden in einem sich ständig vertiefenden und intensivierenden Dialog sämtliche nicht bewusst wahrgenommenen Bedeutungs-Zusammenhänge erschlossen und freigelegt. Die Kunden werden ermuntert, mit eigenen Worten alles zu beschreiben, was ihnen im Zusammenhang mit Ihrer Arbeit und ihrem Wirken einfällt. Dabei eröffnen sich neue und oft überraschende Einblicke in das jeweilige Unternehmen und Wendungen, die dann systematisch auf ihre Relevanz weiterverfolgt werden. Ein Coaching wird so zu einer gemeinsamen Forschungsreise von Psychologe und Securitymanager und eignet sich auch besser zur Kontrolle von Awareness-Maßnahmen als quantitative Verfahren, da sich Security aufgrund der sich ständig ändernden Bedingungen, die vor allem auf den unberechenbaren menschlichen Faktoren zurückzuführen sind, einer klassischen BWL-geprägten Messung widersetzt.

Kreation, Kommunikation & Co.

> Kreation einer unternehmensförderlichen Information Security Umgebung
> Kreation von Awareness-Tools, von Learning Maps sowie von Mitarbeiter-Events und -Incentives
> Verzahnung aller Awareness-Maßnahmen und integriertes Management aller Maßnahmen
> Kommunikation von Awareness-Success-Stories zu PR-Zwecken

Awareness-Tools müssen eine Bilddramatik transportieren und den Mitarbeiter darin als Mitstreiter erfahrbar machen. Die Grundlagenstudie »Entsicherung am Arbeitsplatz« hat gezeigt, dass der Wunsch besteht, menschlich-schräge Seiten in einer zunehmend sachlichen Unternehmenskultur zu erhalten. Eine versachlichende, allzu didaktische oder gar drohende Ansprache der Mitarbeiter ist kontraproduktiv. Sinnliches Einbeziehen in eine dramatische Geschichte ist das, was Awareness erzeugt. Z.B. ermöglicht die Visualisierung von Angreifern (und Verteidigern) und deren Auseinandersetzung, diese als Stellvertreter der im Arbeitsalltag unterdrückten unkultivierten Tendenzen zu nutzen (z.B. wie beim known-sense-»Virusquartett«). Nur belebende Auseinandersetzung bindet die Mitarbeiter ein (Identifikation) und sensibilisiert sie. Darüber hinaus forciert eine nach askit erstellte Visualisierung von Corporate Security Identity, etwa als Learning Map (Comic, Collage, ausschweifendes Ölgemälde, etc., jeweils mithilfe von Grafikern, Malern oder etwa Medienkünstlern), das Verstehen der jeweils analysierten Sicherheitskultur und deren Optimierung.

Die Benefits von askit liegen auf der Hand: Sicherheitskultur wird von Menschen »gemacht« und geprägt - nicht von Maschinen. Und im Umgang mit Menschen sorgt psychologische Kompetenz unumstritten für eine große Wirkung. Eine Begleitung durch ein askit-Coaching fördert z.B. die exakte Analyse von Sicherheitskultur und eine klare Kommunikation aller an Corporate Security beteiligten Personen und Gruppen. Das Wissen um die genauen Ursachen wiederum führt zu höherer Effizienz bei der Kreation von Maßnahmen, d.h. Security-Phänomene werden nicht isoliert betrachtet, sondern im Kontext zu allen relevanten Nebenschauplätzen. Und der Kreationsansatz, der z.B. auf paradoxe Intervention setzt, fördert bei den Mitarbeitern Emotionalität, Zuspitzung und Involvement. Schließlich entsteht Awareness immer nur dann, wenn Menschen sich tatsächlich mit dem zu sensibilisierenden Gegenstand beschäftigen – und dies nicht nur kognitiv, sondern auf allen Wahrnehmungsebenen. ■

askit-Imagefolder (16 S., 72 dpi, 4,9 MB)
http://www.known-sense.de/askit.pdf

Neue tiefenpsychologische Securitystudie mit <kes>

»Aus der Abwehr in den Beichtstuhl – der Securitymanager zwischen Doppelagent und Seelsorger«

Im Rahmen unserer neuen Sicherheitsstudie »Aus der Abwehr in den Beichtstuhl – der Securitymanager zwischen Doppelagent und Seelsorger. Qualitative Image- und Positionierungsanalyse C(I)SO & Co.« werden ca. 30 Sicherheitsbeauftragte in zweistündigen Tiefeninterviews u.a. nach Ihrer Arbeit, ihrer Positionierung, ihren Erfahrungen, Wünschen und Erwartungen befragt. Kern der Studie ist eine Image- und Positionierungsanalyse CSOs/CISOs und die Erstellung einer Typologie »Sicherheitsbeauftragte«.

Hieraus können Learnings für sämtliche Zielgruppen, die im Kontext von Informationssicherheit agieren, generiert werden:

- **Sicherheitsbeauftragte** erhalten einen aufschlussreichen Selbstbild-Fremdbild-Abgleich sowie eine fundierte Analyse der Stärken und Schwächen, aus denen sie Rückschlüsse auf sich, ihre Arbeit und die Sicherheitskultur in Ihrem Unternehmen und deren Optimierung generieren sowie Ihre exakte Positionierung gegenüber Vorgesetzten, IT-Abteilung, Unternehmenskommunikation, Mitarbeitern, etc. herleiten können.
- **Unternehmen und deren Security-Consultants** erhalten bisher weitgehend »verschüttete« tiefenpsychologische Erkenntnisse bzgl. der aktuellen Sicherheitskultur in Unternehmen sowie über den Zusammenhang von Sicherheitskultur und Auftritt wie Positionierung ihrer CSOs/CISOs.
- **IT- und Kommunikationsabteilung** erhalten Anregungen und Handlungsanweisungen zur Optimierung der internen Kommunikation und insbesondere ihrer Kommunikation mit dem Sicherheitsbeauftragten.
- **Entscheider und Personalmanager** erhalten klassifizierte Kriterien zur Beurteilung von CSO-/CISO-Profilen.
- **Security-Dienstleister** – insbesondere Anbieter technischer Lösungen – und Fachmedien erhalten fundierte Informationen über Ihre Zielgruppe und hinsichtlich einer produktiven Ansprache von Sicherheitsbeauftragten sowie IT-Abteilung.
- **Kommunikationsagenturen und Awareness-Dienstleister** wie known_sense können aus den Studienergebnissen Coachings, Kommunikationsbriefings u.a. Tools für Sicherheitsbeauftragte entwickeln, die die oben aufgeworfenen Topics und die spezielle Situation der CSOs/CISOs berücksichtigen und diese darin unterstützen, Positionierung, Kommunikation und Maßnahmen zu verbessern.

Basierend auf Erfahrungen im Awareness-Umfeld kann known_sense über zahlreiche Maßnahmen berichten, die aufgrund fehlender Unterstützung der Sicherheitsbeauftragten scheitern oder gar nicht erst gelaunched werden. Neben der offiziellen Kommunikation existiert in zahlreichen Unternehmen eine non-verbale Ebene, auf der die Belange der Informationssicherheit desavouiert werden. Eine diesbezügliche Kausalanalyse ist Bestandteil dieser Studie. Es ist zu vermuten, dass Entscheider einerseits Maßnahmen der Informationssicherheit als Barriere ihrer Unternehmungen betrachten, dass sich aber andererseits weitgehende Teile der Mitarbeiterschaft hiesiger Unternehmen einem qua Awareness-Kampagne kommunizierten Signal zum Aufbruch und damit erwünschten Veränderungen (Aufwand) verweigern.

CSOs brauchen Story & ein Gesicht!

Learnings über das Wirken der IT-Abteilung allgemein konnten wir bereits in der 2006 produzierten Grundlagenstudie »Entsicherung am Arbeitsplatz«, mit unseren Partnern <kes>, dem DSV, der EnBW, nextsolutions, Pallas und HP ableiten:

- Security-Maßnahmen wird ambivalent begegnet: Einerseits helfen sie (Admins, Sicherheitsbeauftragte) durch ihre administrative Präsenz, die Arbeitsverfassung des Einzelnen im gewünschten Rahmen zu halten. Andererseits werden sie als Exekutive des Systemzwanges im Unternehmen erlebt. In dieser Verkehrung werden sie als Kontrollinstanz mit einem Hang zu Größenwahn und Sadismus beschrieben. In der Regel wird ihnen misstrauisch bis ablehnend begegnet.
- Die IT-Abteilung hat zugleich eine sichernde und eine entsichernde Seite: Als Wissende (z.B. Passwort zurücksetzen) verhilft sie dazu, einen unbewussten Ausbruch ohne die Konsequenz →

eines tatsächlichen Verlustes der Zugehörigkeit überhaupt erst zu ermöglichen.

- Information Security braucht eine Story! Information Security bleibt über weite Strecken unsichtbar und unfassbar. Es zeigt nur wenig sinnliche Ansätze bzw. Szenarien. Security erzählt zu wenig Geschichten. Sie bleibt ein seltsam unbelebter Teil im Unternehmen.
- Information Security braucht ein Gesicht, braucht Protagonisten.
- Information Security nutzt ihr Potential zur produktiven Gestaltung der Unternehmenskultur bislang zu wenig, hat aber die Chance, eine sinnliche Belebung in oft sachliche Zwänge zu bringen und so regulierend auf die Gesamtverfassung des Unternehmens einzuwirken. Sie ist nicht nur Teil der Unternehmenskultur, sie kann die Kultur auch entscheidend prägen.

Kernfragen, die sich aus diesen Erkenntnissen ableiten lassen, müssten also u.a. in etwa lauten: Wie lassen sich die entsichernden Seiten der Information Security, die sich aus sich heraus generieren, reduzieren und die unbelebten bis grauen Images des Sicherheitsbeauftragten aufladen?

Entsicherungen nicht beseitigen

Darüber hinaus können aus der anstehenden Studie auch Learnings für geplante Awareness-Maßnahmen eruiert werden: Der Umgang mit unternehmensbezogenen Sicherheitsmaßnahmen ist wesentlich davon geprägt, wie der Einzelne das Unternehmen als Ganzes, und seine Stellung innerhalb dieser »Arbeitsfamilie« erlebt. Das bedeutet, dass jedes Unternehmen seine individuelle Sicherheitskultur »produziert« und diese somit untrennbar mit der Kultur des Unternehmens verbunden ist. Dies hat Konsequenzen für die Ausrichtung jeglicher Kommunikation, die Sicherheit zum Thema hat:

Entsicherndes Verhalten lässt sich nicht als isoliertes Phänomen verstehen, das es mit allen Mitteln zu beseitigen und verhindern gilt. Vielmehr ist die Frage zu stellen: Welcher Sinn kommt in diesem Verhalten zum Ausdruck? Weiterhin ist zu klären wie sicherheitsbezogene Themen bislang aufgegriffen und dargestellt wurden und welches Bild von Sicherheits- und damit in Teilen auch Unternehmenskultur damit kommuniziert wurde.

Ohne Veränderung null Awareness

Für die Entwicklung einer wirksamen Kommunikation im Bereich Security Awareness durch den Sicherheitsbeauftragten würde dies bedeuten:

- Das grundlegende Zusammenwirken von Unternehmenskultur und Sicherheitskultur muss vom Sicherheitsbeauftragten verstanden werden.
- Zielführend ist die Frage, welche unternehmensspezifische Problematik anhand des entsichernden Verhaltens seiner Mitarbeiter behandelt wird.
- Eine wirksame Security Awareness Kampagne muss die unternehmensspezifischen Motive entsichernden Verhaltens aufgreifen und darüber eine Veränderung einleiten.

Sponsoren wilkommen

Wenn wir Ihr Interesse geweckt haben, sich an dieser erstmals durchgeführten Untersuchung als Partner und Sponsor zu beteiligen, würden wir uns über ein Feedback freuen. Als Sponsor genießen Sie zahlreiche Vorzüge gegenüber »normalen« Käufern der Studie, die sich nicht nur auf das Co-Branding des Berichtsbandes und der erhöhten Aufmerksamkeit durch gemeinsame PR-Aktivitäten erschöpfen. Sie erhalten z.B. Sonderkonditionen bei Mediaschaltungen im unmittelbaren Umfeld der Studien-Berichterstattung unseres Medienpartners <kes> sowie Informationen aus erster Hand. Als Sponsor nehmen Sie VOR dem Launch der Studie an einer zweistündigen Präsentation der psychologischen Projektleiter in Köln teil, die Ihnen auch Hintergrundinformationen und Argumentationshilfen liefern. Darüber hinaus können Sie bei Tiefeninterviews zuschauen, damit Sie sich ein Bild von der Methodik machen können und stehen während der Untersuchung und der PR-Aktivitäten nach dem Launch in einem ständigen Dialog mit unserem Team. Natürlich erhalten Sie zahlreiche Studienbände und -PDFs – wahlweise in deutsch oder englisch – für Ihre Partner und/oder Kunden.

Die Feldarbeit zu unserer neuen Sicherheitsstudie beginnt im Spätherbst 2007. der Erscheinungstermin ist Anfang 2008. Bei Interesse erwarten wir Ihre Anfrage bis zum 15. September 2007. ■

Olé Nr. 7 erscheint im Herbst 2007.

IMPRESSUM

Herausgeber:
Dietmar Pokoyski (known_sense)
Kaiser-Wilhelm-Ring 30-32
D-50672 Köln
Fon +49 221 91277778
sense@known-sense.de
www.virusquartett.de
www.known-sense.de