olé

Der Security-Newsletter
hrsg. von known_sense

11 Dez. 2009

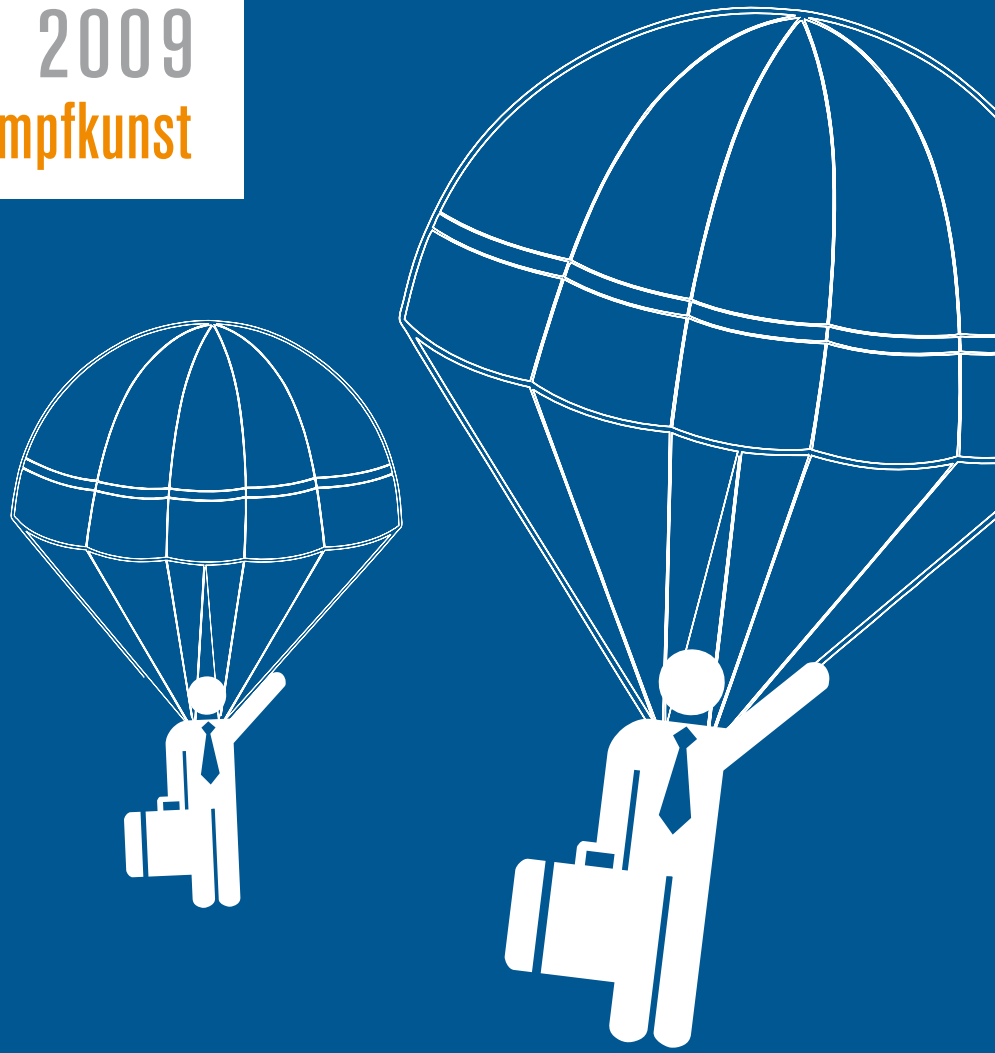
Awareness + Unternehmenskultur + Elektronische Kampfkunst

CISO-Image: Sicherheit im Blick von oben

Neue tiefenpsychologische Security-Studie legt TOP-Management auf die Couch und untersucht die Beziehungen von Entscheidern und Sicherheits-Verantwortlichen

E-Learning-Lösung für Security-Awareness

Bei der Einführung einer Security-Lern-Software gibt es nicht nur eine Möglichkeit



Sicher von oben – Qualitative Imageanalyse CISO & Co. Security Manager und Informationssicherheit aus Sicht von Geschäftsführung, Management und Vorständen. Hrsg. von der EnBW Energie Baden-Württemberg, known_sense und paulus.consult. Förderer Munich Re und ISPIN. Medienpartner eco, <kes> sowie securitymanager.de. 53 S. Euro 380,00/290,00 (für <kes-Abon.). Über known_sense (sense@known-sense.de) oder über den <kes>-Buchshop bestellbar!

Weitere Informationen:

- Studien Summary (11 S., PDF, 72 dpi, 1,3 MB): http://www.known-sense.de/ciso/sicher_von_oben_summary_72dpi.pdf
- Abbildung Cover Berichtsband (JPG, 0,5 MB): http://www.known-sense.de/ciso/sicher_von_oben_cover.jpg
- Abbildung Infografik CISO-Typologie (JPG, 0,4 MB): http://www.known-sense.de/ciso/sicher_von_oben_infografik.jpg
- Auszug CISO-Vorgängerstudie (Selbstbild CISOs) von 2008 (10 S., PDF, 72 dpi, 1,9 MB): http://www.known-sense.de/ciso/securitystudie_auszug.pdf

CISO-Image: Sicherheit im Blick von oben

Tiefenpsychologische Studie legt TOP-Management auf die Couch und untersucht die Beziehungen von Entscheidern und Security-Verantwortlichen

Dietmar Pokoyski

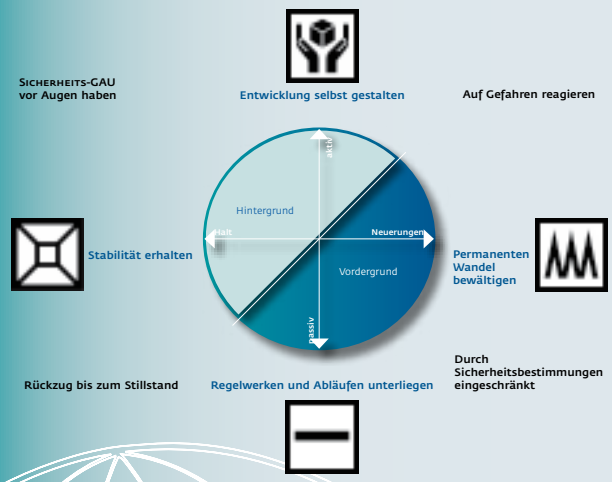
In Köln wurde Ende November 2009 die aktuelle tiefenpsychologische Securitystudie »Sicher von oben – Qualitative Imageanalyse CISO & Co.« von known_sense und den Mitherausgebern EnBW Energie Baden-Württemberg und paulus.consult vorgestellt. Förderer sind darüber hinaus die Munich Re sowie der Schweizer known_sense-Partner ISPIN. Die Ergebnisse unterstreichen wie bereits die der Vorgängerstudien, dass Qualität und Reifegrad von Informationssicherheit in Unternehmen nicht nur durch technische oder organisatorische Faktoren bestimmt werden, sondern in einem erheblichen Umfang auch von der Positionierung des CISO sowie der Kommunikation zwischen ihm und dem TOP-Management abhängen.

Im Rahmen dieser Studie, die von eco – Verband der deutschen Internetwirtschaft, der Zeitschrift für Informations-Sicherheit, <kes>, sowie securitymanager.de als Medienpartner unterstützt wird, wurden 17 deutsche TOP-Manager zwei Stunden lang auf die Couch gelegt und mithilfe von Tiefeninterviews auf Basis der morphologischen Wirkungsforschung zu ihrem Bild von Informationssicherheit und deren Protagonisten (CISO & Co.) befragt. Zu Wort kamen Vorstandsvorsitzende, Vorstände, Geschäftsführer und andere Entscheider, die den Psychologen einen mehr oder weniger tiefen Blick auf den persönlichen Umgang mit den Themenkomplexen Informationssicherheit, Unternehmens- und Sicherheitskultur, Umgang mit sensiblen Daten – beruflich wie privat – sowie auf das CISO-Image und ihre (persönliche) Beziehung zu ihren Security Managern erlaubten.

Wolfgang Reibenspies, Konzernbevollmächtigter IuK-Security der EnBW, sagt über die Beteiligung seines Unternehmens an dieser Studie: »Wenn es um den Informationsschutz im Unternehmen geht, setzt die EnBW auf ein enges Miteinander von TOP-Management und CISO. In Zeiten von knappen Ressourcen und sich stetig ändernden Rahmenbedingungen ist das inhaltliche Verständnis zwischen TOP-Management und CISO das entscheidende Element für nachhaltige Erfolge im Informationsschutz«.

Informationssicherheit von Unternehmenskultur geprägt

Bereits 2006 wurde in einer ersten Grundlagenstudie das Thema Sicherheit und so genannte »Fehlleistungen« aus dem Blickwinkel der Mitarbeiter heraus tiefenpsychologisch aufgegriffen und analysiert. Im Jahre 2008 wurden CISO & Co. zu ihrem Selbstbild, ihrer Arbeitswirklichkeit und zu ihren Visionen befragt. Beide Stu-



dien, die ebenfalls u.a. mit Beteiligung der EnBW stattfanden, brachten grundlegende Erkenntnisse der jeweiligen Positionen zu Tage.

Auch im Rahmen der aktuellen Studie »Sicher – von oben« gelang es, den Einfluss der Unternehmenskultur und der Informationssicherheit auf das Image von CISO & Co. herauszuarbeiten. Darüber hinaus, die zentralen Störstellen der konkreten Zusammenarbeit mit den Sicherheitschefs aus Führungssicht zu identifizieren, eine Typologie der CISO aus Perspektive des TOP-Managements zu entwickeln und diese den Idealvorstellungen und der Selbstsicht der CISOs, die in der Vorgängerstudie beschrieben wurde, gegenüberzustellen.

Kontrollverluste gefährden persönliche Sicherheit

Dabei erwiesen sich die Tiefeninterviews mit den Führungskräften als deutlich schwieriger als die Gespräche mit den CISOs in 2008. Die Manager behalten bevorzugt die Kontrolle über die Gespräche und scheinen wesentlich interessierter an einer persönlichen Absicherung als an der Sicherheit des von Ihnen geführten Unternehmens zu sein. Nicht selten bleiben Antworten bemüht auf hohem Abstraktionsniveau – nur auf Nachfragen wird z.T. demonstrativ auf die Detailebene eingegangen. »Rausgerutschte« Bemerkungen werden nur unwillig erläutert. Ein Einlassen auf individuelle und persönliche Einschätzungen – über (eingeübte) Standardantworten hinaus – erfolgt nur widerstrebend. Empfundene Kontrollverluste, das Offenbaren von Firmeninterna, (sehr) persönlichen Erfahrungen und Einschätzungen führen dabei zu mitunter sehr emotionalen Reaktionen. Es kommt zu einer massiven Abwehr, z.B. in Form von kühlen Verabschiedungen (»Sie finden ja alleine raus.«), Abwertungen der Studie bei vorangegangener Zustimmung (»Und damit wollen Sie also Neues erklären?«) oder zu persönlichen Kränkungen der Interviewer (»Blonde Frauen werden ja im Allgemeinen als sympathischer eingeschätzt.« gegenüber einer dunkelhaarigen Moderatorin).

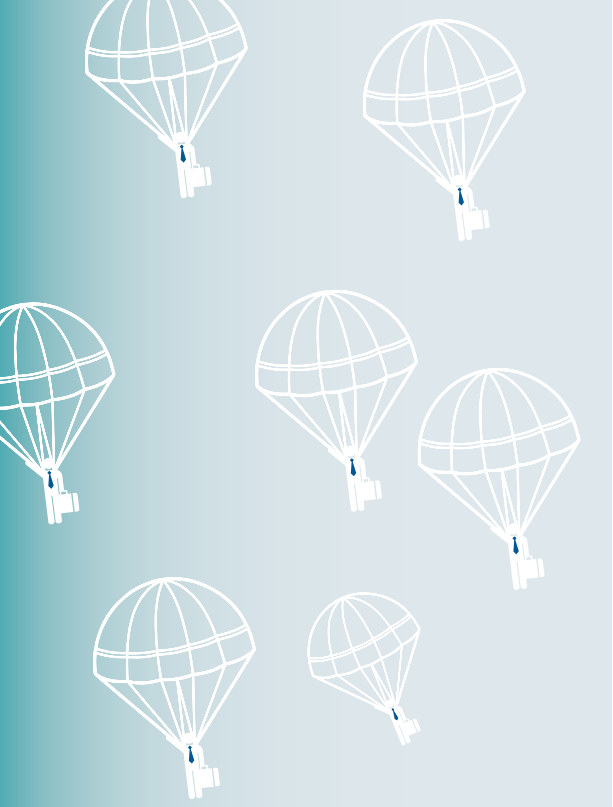
Auf der anderen Seite führten Kontrollverluste aber auch zu deutlich privaten und persönlichen Weiterführungen des eigentlichen Interviews. Die Diplom Psychologin und Projektleiterin der Studie, Ivona Matas, fasst die Erfahrungen der Interviewer wie folgt zusammen: »Die persönliche Sicht der Führungskräfte auf das Thema Informationssicherheit und das Image des CISO stellt sich als deutlich dramatischer und brisanter dar, als es im ersten Zugang von den Managern demonstriert wird.«

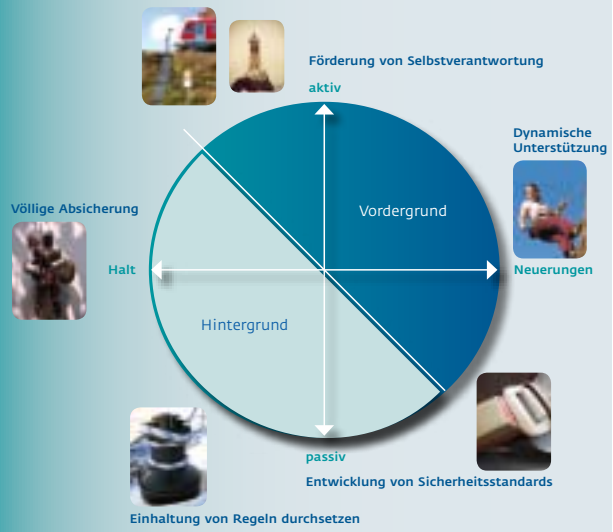
Kommunikation bestimmt Beziehung und Security-Qualitäten

Dabei betonen die Psychologen, dass eine Beschreibung von Positionierung und Kommunikationsqualitäten zwischen Security-chefs und TOP-Managern ohne intensiven Blick auf die jeweilige Corporate Culture kaum möglich ist und stellen fest: Die Unternehmenskulturen befinden sich heute mehr denn je in einer Grundspannung zwischen Stabilität und Innovation. Entscheider positionieren sich aus ihrer Unternehmer-Haltung deutlich auf der Seite der Veränderungen und stellen die aktive Einwirkung auf den Wandel in den Vordergrund. Den notwendigen Halt für die eigene aktive Rolle bieten die erlebte Stabilität der eigenen Position und z.T. auch die eigene Unternehmenshistorie.

Hier kommen Security-Protagonisten und die Informationssicherheit nicht selten als Störer ins Spiel. Als Fortsetzung der Studie von 2008 kann – abweichend von der Selbsteinschätzung der CISOs –konstatiert werden, dass diese vom TOP-Management zwar sehr positiv und respektvoll beschrieben werden; diese Beschreibungen jedoch nur im ersten Zugang Bestand haben! Denn während das Ideal die Security-Protagonisten als kompetenten Unterstützer der Führungskräfte zeigt, werden unter dieser glatten Oberfläche zahlreiche ungeliebte Tätigkeiten an den CISO delegiert, dessen (sicherheitskonformes) Handeln dann nicht selten unternehmerische Aktivitäten stilllegt und so zu großen Spannungen führen kann.

Innerhalb dieser Konflikte sind TOP-Manager stark bemüht, ihre Position zu wahren. Sie reagieren sensibel auf die spezifischen Machtmöglichkeiten der CISOs, die als





Typus »Streiter der Sicherheit«, »Mahnender Kontrolleur«, »Kompetenter Sicherheits-Spezialist« oder »Selbstbewusster Vermittler« (s.a. Infokasten unt.) konkreten Einfluss auf die unternehmerische Tätigkeit ausüben.

Security-Protagonisten und Führungskräfte laufen dabei Gefahr, sich zunehmend ähnlicher zu werden und sich gegenseitig in Machtkonflikten zu blockieren. Dann nämlich, wenn z.B. die Management-Delegation an den CISO in Form ungeliebter Aufgaben überhand nehmen und der Sicherheitsverantwortliche durch die Führung einseitig als Kontrolleur und Strafinstanz vereinnahmt wird.

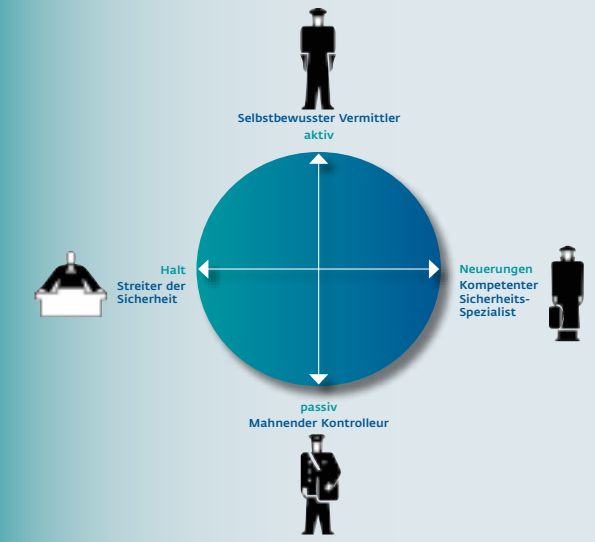
Wolfgang Reibenspies kommentiert: »Insbesondere die Awareness im TOP-Management und vor allem die zielgruppenorientierte Sprache im direkten Dialog sind die größten Herausforderungen für den CISO. Offene und partnerschaftliche Kommunikation steht also im Vordergrund - One-Way-Tickets sind kontraproduktiv!«

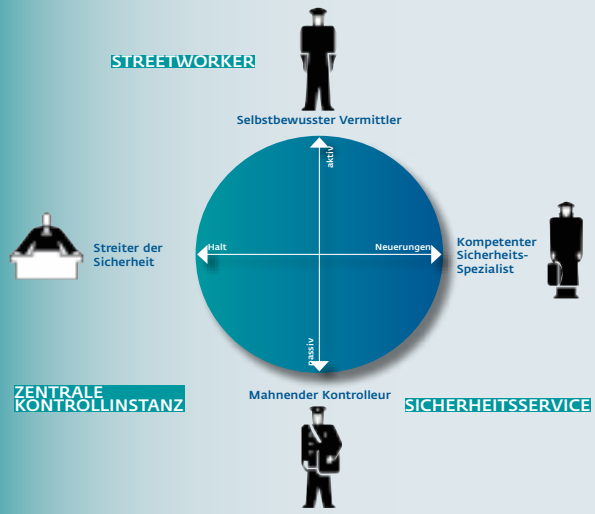
Es fällt auch auf, dass Security-Regeln von den Führungskräften selber nicht eingehalten, aber mit dem Nutzen für das Unternehmen entschuldigt werden. Auch während der Interviews passieren immer wieder Verstöße. So werden die Psychologen z.B. mit internen, nicht weggeräumten Informationen aus Vormeetings konfrontiert oder sollen unbegleitet zum Ausgang finden. Eine Moderatorin findet beim Gang auf die Toilette einen Schlüsselbund samt USB-Stick. In diesem Kontext wird vorzugsweise eine „Lex CEO" kreiert, nach der z.B. Regelverstöße bei Entscheidern und Mitarbeitern unterschiedlich geahndet werden. Damit verfügen Führungskräfte allein aufgrund ihrer Position über andere Lösungsmöglichkeiten bezüglich der (der Informationssicherheit inhärenten) Spaltung als z.B. die befragten Mitarbeiter von 2006 und die befragten CISOs von 2008.

»Die Ergebnisse sind deutlich: CISOs werden von der Geschäftsführung nicht gemocht. Entweder sie sind nicht kommunikativ genug, verstehen das Business nicht, oder sie sind zu mächtig.« sagt Sachar Paulus von paulus.consult und Professor für Unternehmenssicherheit und Risikomanagement an der Fachhochschule Brandenburg. Paulus weiter: »Dies bestätigt meine persönliche Erfahrung und stellt die Erkenntnisse auf fundierte, empirisch belegte Ergebnisse. Nun ist zu überlegen, wie man die Situation verbessern kann. Eine zielgerichtete Ausbildung der Sicherheits-Fachleute ist sicherlich ein wichtiges Element.«

Ivona Matas ergänzt: »Es ist wichtig, Kompetenzen und Aufgaben des Gegenübers eindeutig zu akzeptieren und zu respektieren. Auch seitens des CISO, der offensichtlich zu einer tieferen Einsicht in das Kern-Geschäft seines Unternehmens gelangen muss.« Denn es fällt auf, dass die Führungskräfte einhellig Loblieder über die fachspezifischen Fähigkeiten Ihrer Sicherheitschefs singen, die CISOs aber dieses Lob in punkto Führungsfähigkeiten Ihrer Vorgesetzten oftmals missen lassen.

»Ein professionelles Informationsmanagement wird für den Unternehmenserfolg immer wichtiger. Die zur Verfügung stehenden Ressourcen zum Schutz der Informationen werden dagegen immer knapper«, sagt Michael Lardschneider, Chief Security Officer der Munich Re. Und weiter: »Da die Risiken und Bedrohungen u.a. aufgrund des zunehmenden Wettbewerbs und der Globalisierung wachsen und komplexer werden, ist auch dem Sicherheitsmanagement mehr Bedeutung beizumessen. Entscheidungen im Top-Management bedürfen daher einer fundierten Abwägung der Risiken. Markt- und Liquiditätsrisiken spielen dabei schon lange eine Rolle. Die Betrachtung von Sicherheitsrisiken dagegen ist noch relativ neu. Die Aufgabe, das Verständnis im Top-Management für diese Risiken zu schärfen und im Entscheidungsprozess als Sicherheitsberater zur Seite zu stehen, obliegt dem CSO bzw. CISO. Dass dieser dazu bestimmte Fähigkeiten besitzen muss, um als fachkompetenter Kommunikator und Berater gesehen zu werden, ist für viele Betroffene noch neu. Wie die Studie zeigt, gilt das für beide Seiten, die zu Beratenden (Entscheider) als auch die Berater (CISOs).«





Kompetent streiten, mahnen und vermitteln: Vier CISO-Typen aus Sicht des TOP-Managements

Aus Sicht der Führungskräfte wurden in der aktuellen Studie „Sicher – von oben" insgesamt vier Typen identifiziert, die allerdings in der Realität niemals in Reinform existieren, sondern quasi als eine Cuvee. Dabei existieren für jeden Typus mehr oder weniger gut sichtbare und überwiegend positiv goutierte Hauptbilder, aber auch unter der glatten Oberfläche wirkende Nebenbilder, die deutlich die jeweiligen mit dem Hauptbild (Cover-Story) verbundenen Schwächen (Impact-Story) aufzeigen.

- Der **»Streiter der Sicherheit«** wird als anerkannte und imposante Instanz beschrieben. Im Unternehmen gelingt es ihm, eine breite Vertrauensfront für seine Sache zu kreieren. Auf der anderen Seite tritt er bisweilen als »Bremser« und »Spielverderber« auf, z.B. wenn er auf die Dynamik des Marktes nicht adäquat reagiert und unternehmerische Prozesse zum Erliegen bringt. Der O-Ton einer Führungskraft, »Unser Leiter Security wiegt 150 kg«, macht dies ebenso bildhaft deutlich wie ein zweiter:
»... also eher der kreative Störenfried.«

- Der **»Mahnende Kontrolleur«** zeichnet sich durch Wachsamkeit und Fürsorge aus. Er wittert Gefahren wie z.B. ein Luchs, weil er etwa die Security-Szene – auch als Insider – genau einschätzen kann und daher Risiken kennt, bevor sie einen Namen haben. Darüber hinaus entwickelt er mit großer Leidenschaft Standards, Trainings und sogar komplette Awareness-Kampagnen, leidet allerdings andererseits an einer paranoiden Grundstruktur (»Schnüffler«) mit der Ausprägung, die Darstellung von Sicherheitsrisiken deutlich zu übertreiben. Das Bewahren von Altem steht bei ihm stets vor der Hinwendung zum Neuen.

- Die besondere Stärke des **»Kompetenten Sicherheits-Spezialisten«** ist seine überaus hohe fachliche Kompetenz. Er ist immer auf dem neuesten Stand und unterstützt die Führung darüber hinaus durch seine überbordene Loyalität. Leider entwickelt er manchmal Insellösungen, durch die seine mitunter mangelnden kommunikativen Fähigkeiten bis hin zum »Autismus« deutlich werden. Zwar genießt er bei den Mitarbeitern aufgrund des fachlichen Wissens und Engagements grundsätzlich Respekt, der jedoch in den Darstellungen der Führungskräfte auf der Strecke geblieben ist. »Also wenn die einem dann was erzählen, das verstehen Sie nicht«, sagt eine Führungskraft. »Die müssen in Kundenprojekten mehr von der Realität mitbekommen«, eine andere.

- Der **»Selbstbewusste Vermittler«** verfügt ebenfalls über ein hohes Security-Know-how, hier allerdings gepaart mit den notwendigen kommunikativen Skills, die ihn darin unterstützen, sowohl Mitarbeitern, als auch Führungskräften auf Augenhöhe zu begegnen. Er schafft eine Brücke zwischen Sicherheit und operativem Geschäft und fordert Machtpositionen geradezu ein, gerät hierbei allerdings nicht selten in Konkurrenzsituationen mit der Führung. »Die sind wichtig«, sagt einer. Und …. »Die sind auch ein Riesenproblem… ah, nein, so kann man das jetzt nicht sagen.« Ein anderer Proband stellt fest: »Er vergibt Rechte und steuert Wege … das ist schon eine Machtposition.«

Die hier aus Sicht der Führungskräfte herausgearbeiteten CISO-Typen bieten übrigens durchaus Anknüpfungspunkte zu den 2008 vorgestellten CISO-Selbstbildern und daraus hergeleiteten Typen der Studie »Aus der Abwehr in den Beichtstuhl«. So kann der dort dargestellte Typus der »Zentralen Kontrollinstanz« (Fräulein Rottenmeier) als eine Kombination zwischen den Typen »Streiter der Sicherheit« und »Mahnender Kontrolleur« gesehen werden: Beiden Ausprägungen ist die Einhaltung der Sicherheitsregeln ein Muss.

Der Typus »Streetworker« (Columbo) bleibt nahe beim »Selbstbewussten Vermittler«, indem beiden eine Verbindung von »Analoger Welt« und »Digitaler Welt« gelingt. Der Typus des »selbstbewussten Vermittlers« behält dabei die Anforderungen der Führungskräfte stärker im Blick und verfügt über ein deutlich ausgeprägtes Machtstreben.

Der Typus des »Sicherheitsservice« (Mutter Teresa) rückt stärker zum »Kompetenten Sicherheitsspezialisten«. Wesentlicher Unterschied ist darin zu sehen, dass dem »Sicherheitsservice« ein Abdriften in »Digitale Welten« eher fern ist.

Einführung einer E-Learning-Lösung

Kathrin Prantner

Für die Einführung einer E-Learning-Software gibt es nicht nur eine Möglichkeit. Jedes Unternehmen muss für sich individuell und je nach Ausgangslage und Zielsetzung entscheiden, welche Implementierungsvariante verfolgt wird. Natürlich gibt es Best Practices und Empfehlungen, die einen Überblick über die verschiedenen Möglichkeiten bieten und daher zur Unterstützung herangezogen werden können. Es kann durchaus auch sinnvoll sein, Dienstleister oder auch Hersteller-unabhängige Beratungsleistungen in Anspruch zu nehmen. Teilweise bieten aber auch Hersteller detaillierte Anwendungsszenarien inklusive Anleitungen oder Beratungsleistungen an. Je nach Anforderungen und Komplexität kann eine Lösung auch intern mit eigenen Ressourcen erstellt werden.

Beispiel eines Leitfadens für die Implementierung einer E-Learning-Lösung:

■ Welches Hauptziel wird mit der Einführung der E-Learning-Software verfolgt?

Begleitende oder alleinige Maßnahme, Informationsvermittlung, Bewusstseinsbildung, Tests für Mitarbeiter, Informationsbereitstellung, Überprüfungen, Kostenersparnis gegenüber Schulungen, Reaktion auf einen Vorfall, Anordnung vom Management, Einhalten von Gesetzen und Standards, zeitnahes Lernen, ortsunabhängiges Lernen, attraktives Lernen, Mitarbeiter an das Unternehmen binden, freiwillige Weiterbildung, Mitarbeitermotivation, etc.?

■ Welche Inhalte sollen vermittelt werden?

Unterschiedliche Themen, kritische Themen (z.B. das Sicherheitsverhalten, Verhalten im Brandfall) oder rein informationsbasierende Themen, werden Verhaltensweisen geschult, müssen Verantwortlichkeiten kommuniziert werden, werden Fachinhalte kommuniziert, ist es ein Auffrischungskurs, eine reine Weiterbildung, soll das bestehende Wissen gestärkt werden, ist das Thema trocken und mühsam oder spannend für die Mitarbeiter, etc.?

■ Definition der Zielgruppe?

Ausbildung, Alter, Hierarchie, Abteilungen, Standorte, sprachliche und/oder kulturelle Unterschiede, Wissensstand, unterschiedliche Levels, etc.?

■ Wird eine Lernerfolgskontrolle benötigt/gefordert?

Werden Reporting, Auswertungen, etc. benötigt, wenn ja in welchem Umfang, wird eine personenbezogene oder anonyme Auswertung erwartet, inwieweit wird an das Management reported, gibt es eine unternehmensweite Auswertung, ist die Auswertung Grundlage für eine weitere Aktion, etc.?

■ Gibt es bereits eine Lernplattform im Unternehmen?

Kann ich darauf aufbauen, können Teile verwendet werden, können bestehende und neue Inhalte untergebracht werden, gibt es eine Notwendigkeit für eine Schnittstelle zur neuen Anwendung, etc.?

■ Dauer des Lernprozesses?

Einmaliger Durchlauf, Bestätigung erforderlich, ist das Thema wichtig und muss laufend kommuniziert werden, gibt es verschiedene Lernphasen, etc.?

■ Woher kommen die Inhalte?

Werden diese selbständig kreiert oder können auch vorgefertigte Module gekauft werden, gibt es Inhouse-Experten, etc.?

■ Können andere Abteilungen in den Prozess eingebunden werden?

Kann Unterstützung und Input von anderen Abteilungen angefordert werden, ist es sinnvoll sich mit anderen Abteilungen vorab

Kathrin Prantner absolvierte das Informatikstudium an der Leopold-Franzens-Universität Innsbruck. 2005 war sie Mitbegründerin der E-SEC Information Security Solutions GmbH, für die sie bis heute als Geschäftsführerin tätig ist. E-SEC ist auf Software-Lösungen für Security Awareness spezialisiert und erhielt 2008 für das Produkt E-SEC VIRTUAL COMPANY den Innovationspreis der Initiative Mittelstand. Aufgrund ihres vertrieblich ausgerichteten Aufgabenprofils bei E-SEC steht Prantner in einem ständigen Kontakt zu Security Awareness Protagonisten wie z.B. Sicherheitsbeauftragten sowie zu Anwendern, den Mitarbeitern, in deutschen, österreichischen und schweizerischen Unternehmen.
www.e-sec.eu

Auszug aus: Prantner, Kathrin: Awareness und Lernen. Erstveröffentlichung in: Helisch, Michael und Pokoyski, Dietmar (Hrsg.): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg + Teubner, 2009. (Mit freundlicher Genehmigung des Verlags) 317 Seiten, 49,40 EUR. ISBN: 978-3834806680.

abzustimmen, gibt es vielleicht auch Regelungen, Inhalte, die diese an die Mitarbeiter kommunizieren wollen/müssen, etc.?

- Wer ist für die Einführung der Software verantwortlich?

Sind ausreichende Ressourcen (qualitativ und quantitativ) vorhanden, ist es möglich eine interne Projektgruppe für die Einführung zusammenzustellen, etc.?

- Welche Erfolgsfaktoren werden definiert?

Wann ist der Einsatz erfolgreich verlaufen, können jetzt schon Erfolgsfaktoren definiert werden, wer überprüft den Erfolg, wer entscheidet ob erfolgreich oder nicht, etc.?

- Müssen eventuell gesetzliche Vorlagen oder unternehmensinterne Richtlinien berücksichtigt werden?

Wenn ja, mit welcher Konsequenz für die Einführung, etc.?

- Welches Budget steht zur Verfügung?

Können Ressourcen, Beratung, Lizenzen, Hardware, etc. zusätzlich angeschafft werden, inwieweit ist es günstiger, eine Software zu kaufen oder externe Beratung in Anspruch zu nehmen, kann ich den Aufwand und die Kosten eventuell mit anderen Abteilungen teilen, etc.?

- Rechnet sich die Anschaffung bzw. Einführung einer E-Learning-Software?

Welche bisherigen Kosten würden sich minimieren, Nutzen und Kosten der bisherigen Vermittlungsart, mit welchen Folgen wäre zu rechnen, wenn keine Software eingeführt werden würde, in welchem Verhältnis stehen technische Features und Qualität der Software, welche Vorteile hat die Einführung, hat es neben den Mitarbeitern auch positive Auswirkungen nach außen bei Kunden, Partner, etc., kann ich eine höhere Mitarbeiterbindung, mehr Loyalität erreichen, was sind die direkten und indirekten finanziellen Vor- und Nachteile, etc.?

- Wird ein Autorentool benötigt?

Besteht der Anspruch auf selbständige Wartung der Software, wird die Software intern konfiguriert (Inhalte, Animationen, etc.), welche Features werden zusätzlich benötigt, etc.?

- Welche Hardware steht zur Verfügung?

Reicht dies für die zur Auswahl stehenden Produkte, müssen Lizenzen z.B. Datenbanklizenzen nachgekauft werden, reicht die Bandbreite, etc.?

- Welche Features werden auf keinen Fall benötigt?

Kann ich die Auswahl aufgrund der nicht benötigten Features bereits eingrenzen?

- Falls erforderlich, wie kann der Einführungsprozess einer E-Learning-Lösung kommunikativ unterstützt werden?

Z.B. Poster, Ankündigungen, Ausschreibungen, zusätzliches Informationsmaterial, Gewinnspiele, integrierte Kommunikationskampagne, etc.?

- Gibt es ein offizielles Commitment des Top Managements?

Zusätzliche Tipps

Einigen Sie sich innerhalb Ihres Unternehmens bezüglich der Grundspezifikation und der zu erreichenden Ziele. Es macht Sinn, einen Katalog mit detaillierten Auswahlkriterien zu erstellen. So können Sie die Suchkriterien für ein Produkt erneut einkreisen und auch gezielt nach Produkten und Beratungsleistung suchen, aber auch z.B. eine interne Projekt- bzw. auch Umsetzungsgruppe zusammenstellen.

Für jedes Unternehmen und die für Informationsvermittlung verantwortlichen Personen gilt zu jedem Zeitpunkt folgender Leitsatz: Überprüfen Sie kritisch die eigenen Kompetenzen (fachliche UND pädagogische Kompetenzen) und ziehen Sie bei Lücken interne wie externe Hilfe hinzu. Stellen Sie in jedem Fall ein kompetentes und motiviertes Team zusammen, das sich zum Ziel setzt, einen erfolgreichen Lernprozess einzuführen.

Die im Unternehmen für die kommunikative Implementierung der E-Learning-Software verantwortlichen Personen sollten zu den anerkannten Meinungsführern im Unternehmen gehören. Unterstützung, z.B. über eine eventuell zusätzliche Anordnung einer höheren Managementebene, trägt beim Launch in jedem Fall zu einer positiven Ausstrahlung auf das Produkt und auf das Vorhaben bei.

Sollten keine offensichtlichen Anhaltspunkte bezüglich des aktuellen Sicherheitswissensniveaus der Mitarbeiter existieren, können persönliche Umfragen und Gespräche Sie darin unterstützen, die Lücke zu schließen. Im Zweifelsfall sollten Sie auch hier auf externe Unterstützung zurückgreifen, z.B. auf professionelle Umfragetools oder auf qualitative bzw. quantitative Evaluationen.

Bewertung div. didaktischer Tasks im Rahmen von Security Awareness

TASK	LERNEN	E-LEARNING	TRAINING
Erweiterung Wissensstand	+	+	+
Weiterbildung	+	+	+
Messbarkeit des Lernerfolges	+	+	+
Lernkontrolle	-	+	+
Reaktionszeiten auf Neues	-	+	+
Rollendefinition	~	+	+
Mitarbeitermotivation	-	~	+
Asynchron	~	+	+
Zeitunabhängig	-	+	+
Ortsunabhängig	-	+	+
Lernen aus Distanz	-	+	+
Dokumentation Lernfortschritt	~	+	+
Wiederholung von Inhalten	~	+	+
Eigenes Lerntempo	-	+	+
Aufbauend auf Wissenslevel	~	+	+
Erreichbarkeit aller Lerntypen	-	+	+
Animation	-	~	+
Interaktivität	-	~	+
Selbstdisziplin	~	~	~
Bewusstseinsbildung	-	-	+
Ausführen von Tätigkeiten	-	-	+
Bezug zum realen Leben	~	~	+
Abläufe automatisieren	-	-	+
Reporting	-	+	+
Organisationsaufwand	~	~	~
Kombinierbar mit anderen Lernformen	+	+	+
Generationenunabhängig	~	~	~
Umsetzung Interkulturelle Unterschiede	~	+	+
Geschlechterunabhängig	+	+	+

Legende: + positiver Effekt ~ neutral bzw. von anderen Faktoren abhängig - negativer Effekt

Die wichtigsten Fakten für E-Learning zusammengefasst:

Zusammenfassend kann gesagt werden, dass E-Learning ein durchaus zielorientierter und effizienter Kanal ist, um Security Awareness unternehmensintern zu vermitteln. Des Weiteren wurde deutlich, dass auch Security Awareness Next Generation von adäquaten E-Learning-Lösungen profitieren kann und umgekehrt. Folgende Auflistung beschreibt die wichtigsten Do's und Dont's, die bei Einsatz einer E-Learning-Lösung zu berücksichtigen sind, sowie Vor- und Nachteile:

- E-Learning ermöglicht, individuelle Bildungsziele zu verwirklichen. Die individuellen Bedürfnisse und Ziele des Lernenden können stärker als im Rahmen von Präsenztrainings berücksichtigt werden.
- Orts- und zeitunabhängiges Lernen – überall, wo zumindest ein Computer allenfalls mit Internetanschluss – zur Verfügung steht, ist »Lernen aus der Distanz« möglich. Lernender und Lehrender müssen nicht mehr zur selben Zeit an einem Ort zusammentreffen, um miteinander zu kommunizieren.
- Der Lernstoff kann selbständig wiederholt werden. Das Lerntempo erfolgt nach individuellem Bedürfnis und kann den Vorkenntnissen entsprechend angepasst werden.
- Hochwertige E-Learning Security Awareness Lösungen liefern ein messbares Ergebnis in punkto sicherheitsrelevantem Wissen. Des Weiteren inkludiert eine Lösung meist Reporting-Funktionalität, wodurch der Wissenslevel der Mitarbeiter zu jedem beliebigen Zeitpunkt ausgewertet und dokumentiert werden kann.
- Selbst das raffinierteste E-Learning-Produkt erspart niemandem das Lernen. Lernen bleibt nach wie vor ein individueller Prozess, der von den Lernenden selbst ausgehen und von ihnen geleistet werden muss.
- Im E-Learning-Bereich gibt es eine Vielfalt von Anbietern unterschiedlichster Produkte. Ein einheitlicher Qualitätsstandard fehlt aber bislang. Die Praxis zeigt, dass die Qualitätsunterschiede zum Teil sehr groß sind und manche Produkte weit hinter den Erwartungen zurück bleiben.

Fazit

Bei Lernen wird davon ausgegangen, dass die Mitarbeiter mittels Lernmaterialien und begleitenden Veranstaltungen, die durch Lehrende abgehalten werden, lernen. Beispiele dafür sind: Weiterbildungskurse, Fachkurse, Schulungen, Unterweisungen, etc.

Bei E-Learning wird vom Einsatz einer klassischen E-Learning-Software ausgegangen (Kontent Providing). Training inkludiert die Bereitstellung von Trainings und Übungen bzw. Nachahmung von Situationen mittels Interaktivität und Animation.

Quer durch die IT-SA

Beim Mitmach-Riesenspiel »Quer durch die Sicherheit« wurden die Messebesucher der II-SA spielerisch in Awareness-Kontexte involviert

Im Rahmen der IT-SA, die 2009 erstmalig als eigenständige Messe in Nürnberg stattfand, hatten die Besucher am aware-house-Stand die Möglichkeit, das known_sense -Securitygame »Quer durch die Sicherheit« auszuprobiere und im Wissens-Wettstreit gegeneinander anzutreten (s. Abb. l. u. r.).

»Quer durch die Sicherheit« ist ein lehrreicher wie unterhaltsamer Mix aus Security-Quiz- und Zug-um-Zug-Strategiespiel. Basierend auf 49 50x50cm großen Quizkarten mit Fragen zum Thema sowie mithilfe von überdimensional großen Würfeln und Spielfiguren entstand ein begehbares und ca. 20 qm großes Riesenspiel, bei dem die Mitspieler jederzeit auch die Spielfiguren ersetzen können, um Teil des Spiels zu werden.

Nach der EnBW setzt nun auch die Schweizer ISPIN AG das Riesenspiel für Schulungen und im Rahmen von Security-Events ein. Weitere Unternehmen haben für 2010 einen Ankauf oder die Anmietung angekündigt. Auch die kleinere, nur ca. 100 x 100 cm große Tischversion kann jederzeit auch im eigenen Firmen-Brand via known_sense lizensiert werden.

http://www.known-sense.de/quer_durch_die_sicherheit_folder.pdf ■

Virtual Training Company in 2010 bei aware-house

Das E-SEC-Awareness-Tool »Virtual Training Company« wird 2010 als aware-house-edition inkl. Tools und Know-how für CISO & Co. verfügbar sein. ■

Wölfe & Geißen im März 2010

Der Rheinische Security Roundtable »Wölfe & Geißen« wird im März 2010 zum 11. Mal stattfinden und dann von dem Kölner Unternehmen Csecure gesponsert werden. Termine unter www.wolefegeissen.de ■

Moderationsbox

Gemeinsam mit HECOM Security Awareness Consulting hat known_sense soeben den redaktionellen Teil einer Security-Moderationsbox fertig gestellt, die 2010 international für eine fünfstellige Zahl von Führungskräften ausgerollt wird. ■

Security-Podcasts

Im Februar produziert known_sense für einen internationalen Spezialchemikalienhesteller 8 Security-Awareness-Podcasts in 6 Sprachen. Hierfür wird eine bereits im Rahmen von Comics genutzte Leitfigur der laufenden Awareness-Kampagne verlebendigt, indem sie eine Stimme erhält. Mehr über das Projekt, das mit internationalen Sprechern in den Kölner Horchposten-Studios produziert, wird in OLE Nr. 12. ■

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