olé

Der Security-Newsletter
hrsg. von known_sense

8 Mrz. 2008

Awareness + Unternehmenskultur + Elektronische Kampfkunst

Neue Security-Studie:
Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co.

IT-Sicherheitspreis NRW geht an known_sense:
askit – awareness security kit ausgezeichnet

Musée de Sécurité:
Mobile Ausstellung als Roadshow für Security-Events und Awareness-Kampagnen

Beichtvater, Froschkönig oder Columbo?

Selbstbild, Image, Wirkung und Visionen von CISOs im Fokus tiefenpsychologischer Forschung – neue Security-Studie nimmt Sicherheitsverantwortliche unter die Lupe

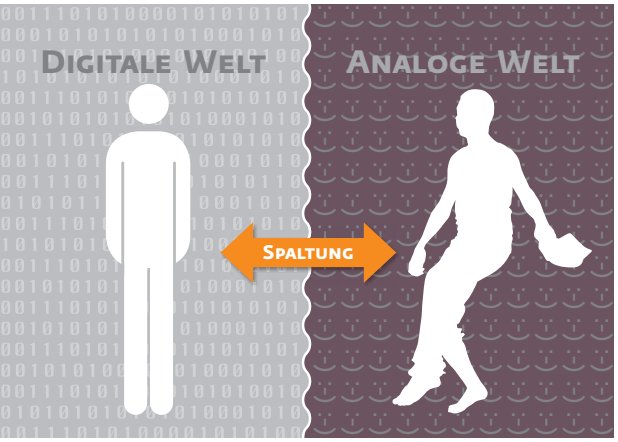
Woher komme ich? Was bin ich? Wo gehe ich hin? Mehr noch: Auf welche Weise? Auf welchen Wegen? Die während der cebit von der EnBW, known_sense, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro publizierte tiefenpsychologische Security-Studie ‚Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co.' zeigt, dass sich die existenziellen Fragen der Sicherheitsverantwortlichen auf den ersten Blick nicht von den klassischen Reflexionen anderer Berufstätiger unterscheiden. Dennoch steckt im Detail das große Besondere, das gerade Sicherheitsverantwortliche so unverwechselbar macht – etwa die paradoxe Anforderung, mit der CISOs (Chief Information Security Officers) in ihrer Arbeit konfrontiert werden. Sie agieren in einer Spaltung, weil sie spüren, dass Sicherheitsrisiken eingegangen werden müssen, um insgesamt für eine stabilere Sicherheitskultur zu sorgen. Denn – das zeigt die aktuelle Forschung ebenso wie die Vorgängerstudie ‚Entsicherung am Arbeitsplatz' – Entsicherungen produzieren Sicherheit. An welchen Stelle jedoch Entsicherung vertretbar ist, hängt von der jeweiligen Strategie des CISOs ab und z.B. davon, ob eher der Typus »Columbo«, der Typus »Mutter Teresa« oder der Typus »Fräulein Rottenmeier« ausprägt ist.

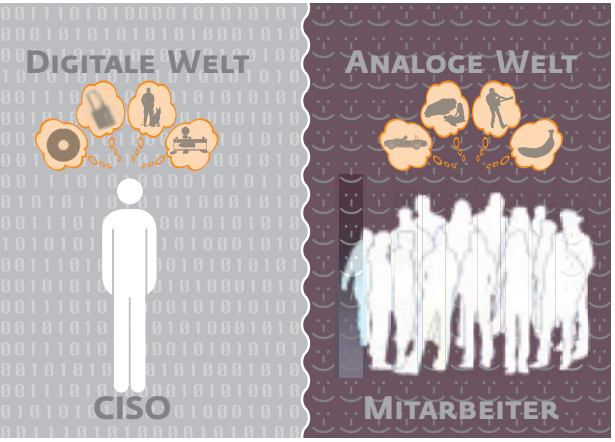
Zunächst reagierten die meisten Probanden allerdings recht ungläubig auf das Forschungsvorhaben. »Was? Es interessiert sich jemand für unseren Beruf«, heißt es in der Regel erstaunt beim Erstkontakt der Sicherheitsbeauftragten mit den Psychologen. Andererseits wird aber auch ein ausgesprochenes Mitteilungs- und Verstehensbedürfnis der CISOs spürbar. »Es fällt auf«, berichtet die Projektleiterin, Diplom-Psychologin Ankha Haucke, »dass die Probanden durchaus mit einem Anliegen in das Interview kommen. Fast alle scheinen etwas über sich und ihren Berufsstand sagen, aber auch erfahren zu wollen.« Man wolle sich offenbar als CISO behaupten, erhoffe sich eine Würdigung des eigenen Handelns und zeige gleichzeitig eine deutliche Neugier zur Sichtweise anderer. Ein O-Ton: »Ich bin sehr gespannt auf das Interview. Es soll ja wohl mehr um das Persönliche beim Job gehen. Vielleicht kann ich zu der Sache beitragen und hinterher auch erfahren, wie es anderen damit ergeht.«

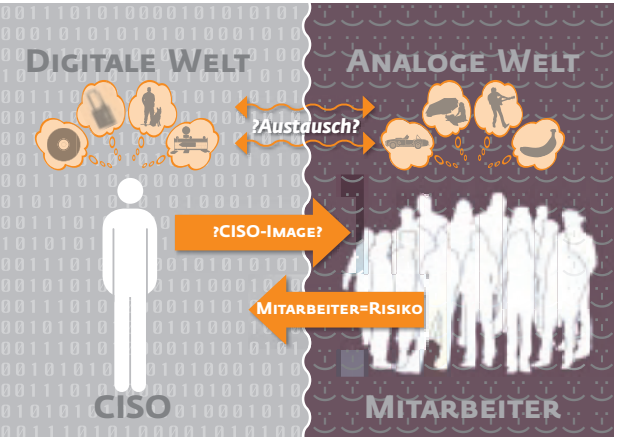
Als Schwierigkeit ihrer Aufgaben sehen viele CISOs, selber nichts Konkretes zu produzieren, das vorzeigbar wäre und an dem man die eigene Wirksamkeit erleben und demonstrieren könnte. IT-Sicherheit ist zwar unbestritten notwendig, erzeugt aber keinen offenkundigen Mehrwert. Eine frustrierte Aussage lautet: »Selbst die Putzfrau trägt dazu mehr bei, indem sie dafür sorgt, dass das Gebäude nicht schmutzig ist und die Kunden sich wohl fühlen.«

Leiden im Untergrund

Diese Unzufriedenheit überrascht nicht: CISOs, das zeigt die Studie deutlich, werden als Vertreter einer anderen, einer unbekannten und unfassbaren Welt mit eigener Sprache und Ordnung betrachtet. Diese Sonderstellung geht mit einer gewissen Form der Entrückung vom Unternehmensbetrieb einher. Die Herkunft des CISOs lässt sich als ‚Digitaler Untergrund' bezeichnen. Die Tätigkeit als CISO und damit das Abtauchen in den Untergrund führt teilweise zu einer Digitalisierung menschlich-paradoxer Verhaltens- und Erlebensweisen der Sicherheitsverantwortlichen. Spontanes, Impulsives, Hitziges, →







Triebhaftes, Menschliches hat hier offenbar kaum noch Platz.

Mitarbeiter denken in Geschichten

Während die Mitarbeiter in Wirkungen, Bildern und Geschichten denken, so die Studie, und hiermit ein ‚analoges Prinzip' pflegen, ist der CISO beauftragt, die Gesamtheit der Unternehmensprozesse in Sicheres und Gefährliches zu ordnen. Was aus Sicht des CISOs ein Risiko darstellt – z.B. das (Zwischen-) Menschliche –, bedeutet für den User umgekehrt Inspiration und Förderung der Arbeitsfähigkeit. Der CISO sieht sich nämlich mit der Aufgabe konfrontiert, eher ein ‚digitales Prinzip' umzusetzen und zugleich einen Umgang mit den gegensätzlichen, menschlich-paradoxen Tendenzen zu finden. Dies führt zu einer inneren Spaltung des CISOs, so dass die Mitarbeiter zu ihm entweder ängstlich auf Distanz gehen oder aber ihn und sein Anliegen nicht ernst nehmen. Der CISO hat dann häufig das Gefühl, wie ein Sonderling behandelt zu werden: »Ich bin die ärmste Sau im Betrieb. Freunde habe ich da nicht«.

Grundproblem des CISOs: Austausch mit der Wirklichkeit

Die Sicherung gegen Angreifer von außen scheint also für den CISO weniger ein Problem darzustellen als der gleichberechtigte Austausch mit den eigenen Mitarbeitern. Sein Grundproblem ist nicht das Leben im ‚digitalen Untergrund', sondern der Austausch mit der ‚analogen Wirklichkeit'.

Vor dem Hintergrund des Umgangs mit diesem Grundproblem beschreibt die Studie unterschiedliche (menschliche) CISO-Strategien, die wiederum unterschiedliche Wirkungen im Unternehmen hinterlassen und zahlreiche bekannte Images und eben Typen zu Tage fördern. Durch die Typisierung der CISOs lässt sich die Lösung des Grundproblems darstellen, wobei die Psychologen betonen, das sämtliche Typen nicht in der dargestellten Reinform existieren, sondern als ‚verschiedene (strategische) Gesichter' eines CISOs zu verstehen sind. Das so genannte ‚digitale Prinzip' wird durch den eher divenhaften Typus ‚Zentrale Kontrollinstanz' alias ‚Fräulein Rottenmeier' repräsentiert, das ‚analoge Prinzip' durch den ‚Sicherheits-Service', der sich durch ein ‚Helfer-Syndrom' (‚Mutter Teresa'), auszeichnet. Der dritte Typus ‚Streetworker' (oder auch ‚Columbo') versetzt sich in die Lage der Mitarbeiter und versucht, seine Interessen auf dieser Ebene zu vermitteln. Er entsichert sich sogar selbst, weil er durchaus bereit ist, Risiken in Kauf zu nehmen, um der analogen Sichtweise der Mitarbeiter zu begegnen. Er lebt das Paradox. Diese Strategie setzt – anders als die die beiden anderen – nicht auf Spaltung, sondern auf ein Verzahnen der beiden unterschiedlichen Prinzipien. Das vermittelnde Verhalten erzeugt Eigenart und Profil, Akzeptanz und Loyalität. Dr. Kurt Brand, Geschäftsführer der Pallas GmbH sagt: »Aus der Studie habe ich gelernt, dass die IT-Security auf drei Beinen steht: Technik, Organisation und Unternehmenskultur. Gerade die kulturelle ➔

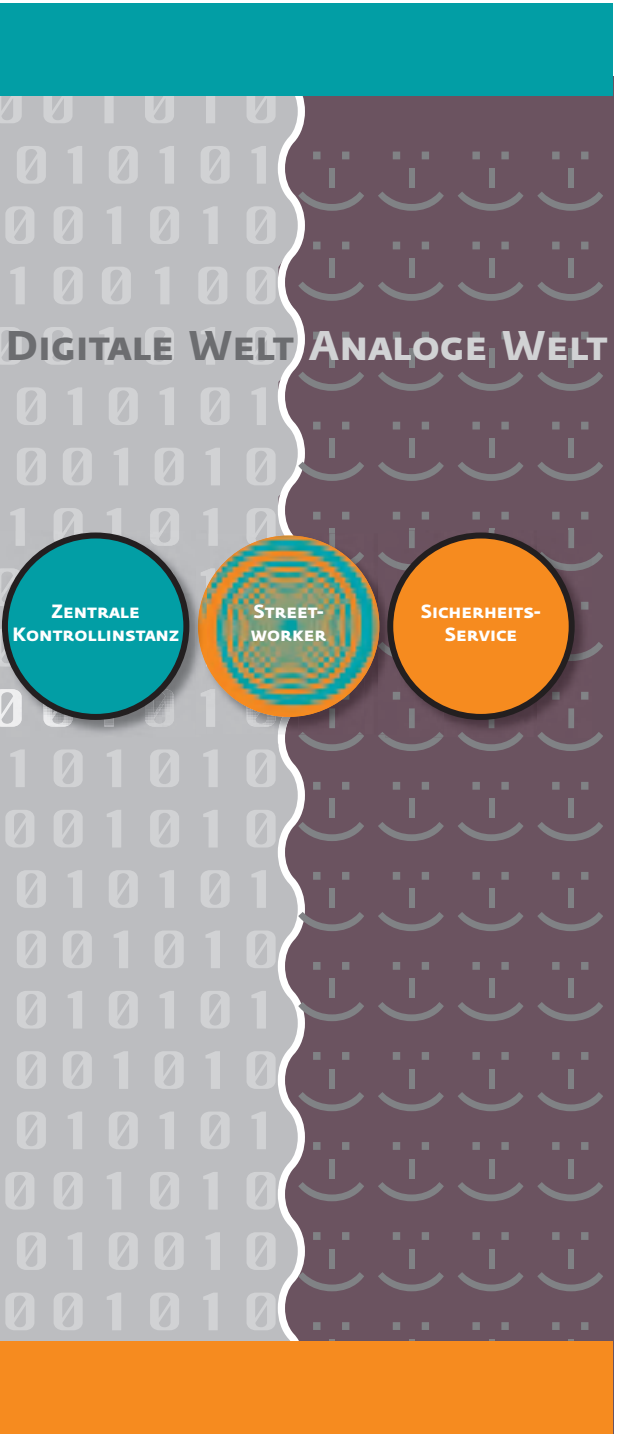
Drei CISO-Typen

Digitales Prinzip – die ‚Zentrale Kontrollinstanz' oder Fräulein Rottenmeier

Die Prozesse laufen, wenn er will, und er scheint unersetzbar. Alles dreht sich um ihn – dennoch ist er einsam. Sicherheitskultur wird durch ihn nicht vermittelt, sondern erzwungen. In dem Typus ‚Zentrale Kontrollinstanz' sind Züge einer Diva enthalten. Man rechnet mit wechselnden Stimmungen und versucht, ihm, der oft unnahbar erscheint, alles recht zu machen. »Wenn der CISO der beliebteste Mann im Unternehmen ist, stimmt etwas nicht«, so ein O-Ton der zentralen Kontrollinstanz. Menschlich-analoge Seiten werden von ihm konsequent abgespalten, um sich nicht zu »beschmutzen« oder sich auf andere Sichtweisen einlassen zu müssen, vergleichbar der literarischen Figur des Fräulein Rottenmeier aus ‚Heidi'.

Analoges Prinzip – Der ‚Sicherheits-Service' oder Mutter Teresa

Dieser Typus möchte, dass Sicherheit nicht in unangenehmer Weise spürbar ist. Seine Freundlichkeit kann aber in Aggression kippen, wenn die Mitarbeiter allzu ungesichert agieren. Dann kann der ‚Sicherheits-Service' Freiheiten sofort einschränken. Probleme und Störungen sind sein Lebenselixier, die seine Rolle als helfender Engel manifestieren. Auch, wenn er sich gut in die User hineinversetzen kann, schafft er es oftmals nicht, die Relevanz seiner Belange durchzusetzen. So fürchtet er letztlich doch um seine Existenz im Unternehmen, z.B. durch die vermeintliche Bedrohung durch externe Security-Sevice-Anbieter. »Ich komme mir vor wie ein Mann vom ADAC. Den holt man auch nur, wenn man am Straßenrand liegen geblieben ist«, sagt einer, ➔



Komponente prägt dabei das Wirken des CISO. Mich beschäftigt nun, wie ich den CISO dabei unterstützen kann, seine Wirksamkeit wahrnehmbar zu machen. Dazu liefert die Studie eine ordentliche Menge Stoff.«

Prinzessin oder Frosch

Im Fazit der CISO-Studie beschreiben die Psychologen eine Analogie zum ‚Froschkönig'. Der Umgang zwischen Prinzessin und Frosch bebildert ein Gefüge, das der Situation des CISOs ähnelt. Nach diesem Prinzip werden zwei zueinander gehörende Seiten als getrennt voneinander dargestellt. Und dennoch drängt eine (unsichtbare) Kraft auf einen Austausch. Der Psychologe Udo Eichstädt sagt: »Die Prinzessin steht dabei für das rein Digitale, das Unnahbare, den Eindruck des Besonderen, kultiviertes Verhalten, Kontrolle und ‚unbedarfte' User – der Frosch symbolisiert banale Wirklichkeit, versteckt in seiner eigenen Welt, aber zugleich hilfsbereit, und außerdem Mitarbeiter, die nur die analoge Perspektive leben.«

Die Psychologen wünschen sich analog zum ‚Froschkönig' für die Konstruktion wie auch für die Vermittlung von Sicherheitskultur einen stärkeren Austausch und Wandel zwischen ‚analogem' und ‚digitalem Prinzip'. Darüber hinaus betonen sie die Notwendigkeit von Führung, Involvement und einer Übersetzung von Sicherheitsthemen zugunsten eines breiteren Verständnisses auf Seiten der Mitarbeiter. In diesem Zusammenhang empfehlen sie den berühmten Blick von außen. Mittel können z.B. ein intensiverer Austausch mit Kollegen sowie speziell für CISOs entworfene Kommunikationsbriefings oder Coachings sein.

Modernes Sicherheitsmanagement mit strategischen Vorgaben

»Die Studie zeigt, dass das Verhalten der CISOs nicht nur rational, sondern auch durch emotionale Impulse bestimmt wird«, sagt Wolfgang Nickel, Senior Manager Competence Center IT-Security Steria Mummert Consulting AG. Und weiter: »Ein modernes Sicherheitsmanagement basiert auf strategischen Vorgaben und führt zu geplantem Verhalten mit messbaren Ergebnissen. Der Aufbau eines Sicherheitsmanagementprozesses steckt in vielen Unternehmen noch in den Kinderschuhen und ist auch mit Blick auf Compliance Anforderungen dringend voranzutreiben.«

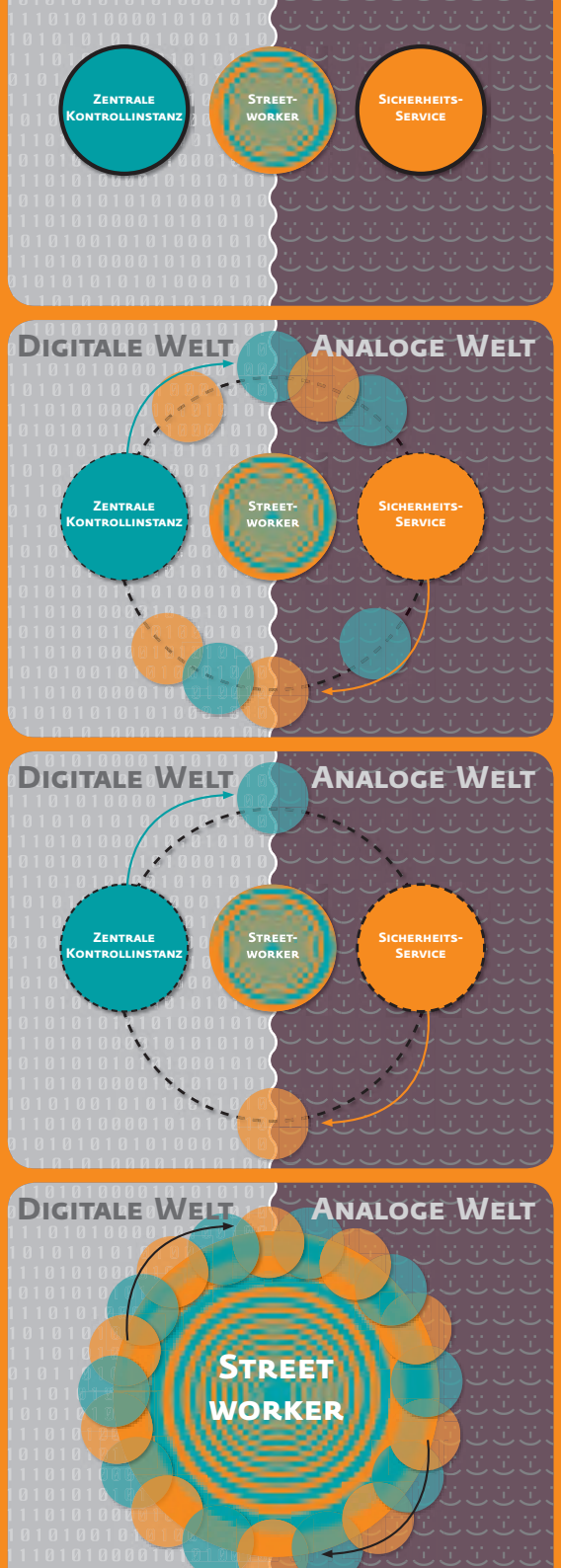
CISO als Marke

Profilierung und Aufmerksamkeit durch professionelle Kommunikation bilden einen weiteren Baustein im Puzzle um das Ringen nach Wirksamkeit der Security: »Wirksame und nachhaltige Sicherheit heißt nicht nur, dass man die Compliance erfüllt«, schreibt Dietmar Pokoyski, Geschäftsführer der Kommunikationsagentur known_sense und Initiator dieser Studie, den CISOs ins Pflichtenheft: »CISOs müssen es schaffen, ➔

oder: »Ich bin nicht der, der die Blondine als Belohnung bekommt« ein anderer. Als Person ist der ‚Sicherheits-Service' wohl am ehesten mit Mutter Teresa vergleichbar.

(Ein-)Beziehung bietet Sicherheit – ‚Der Streetworker' oder Columbo

Er versteht Sicherheit nicht als Lösung von der Stange, sondern als eine individuelle Konfiguration. Seine Strategie zeichnet sich durch Beweglichkeit und seinen Wunsch nach interdisziplinärem Austausch aus. Interessen der Sicherheit und die der Mitarbeiter werden miteinander in ein Verhältnis gebracht. Beim ‚Streetworker' wird der Versuch deutlich, sich in den anderen hineinzuversetzen, ohne die eigenen Belange aufzugeben. »Mein Vorsatz ist: Vergiss nie, dass du auch mal da gesessen hast, wo die jetzt sitzen.« Im Mittelpunkt des Handelns steht das Prinzip der Führung mit Sinnstiftung durch das Einrichten einer Sicherheitskultur. Durch diese Einbeziehung gerät der Mitarbeiter in die Lage, seine eigene (analoge) Perspektive in die (digitale) Perspektive der Informationssicherheit zu überführen.
Der CISO versetzt sich laut Studie wie ein Streetworker in die Lage der Mitarbeiter und versucht, seine Interessen auf dieser Ebene zu vermitteln. In gewisser Weise entsichert sich der ‚Streetworker' sogar selbst, weil er durchaus bereit ist, Risiken in Kauf zu nehmen, um der analogen Sichtweise der Mitarbeiter zu begegnen. Er lebt das Paradox. Er hält es aus, anstatt es zu verbannen. Diese Strategie setzt – anders als die die beiden anderen – nicht auf Spaltung, sondern auf ein Verzahnen der beiden unterschiedlichen Prinzipien. Das vermittelnde Verhalten erzeugt Eigenart und Profil, Akzeptanz und Loyalität und entspricht z.B. am ehesten der bekannten Figur Inspektor Columbo aus der gleichnamigen TV-Krimi-Serie. ■



in Ihrem Unternehmen eine Marke zu bilden. Gerade internes IT- oder Security-Marketing kann, wenn Sicherheit lebendig visualisiert wird, hohes Involvement schaffen. Und eine gute Awareness-Kampagne ist stets auch ein Pro-CISO-Marketing.« ■

Für die Studie »Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co.« wurden insgesamt 30 Sicherheitsverantwortliche aus Nordrhein-Westfalen in einem Studio in Köln oder innerhalb von Office-Interviews on Location mithilfe morphologischer Markt- und Medienforschung befragt. Die Probanden verantworteten jeweils einen eigenen Etat für die Sicherheit in ihrem Unternehmen. Die psychologischen Tiefeninterviews dauerten jeweils 2 Stunden und wurden mit Vertretern aus Unternehmen zwischen 50 und 110.000 Mitarbeitern geführt (gerundeter Durchschnitt aller Firmen 20.000 Mitarbeiter).

Ziel der von EnBW, known_sense, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro verantworteten Forschung war die Darstellung und Erforschung des CISO-Berufsbilds, wobei hierunter leitende IT-Sicherheitsbeauftragte und verwandte Berufsvertreter zu verstehen sind. Dabei ging es nicht wie in quantitativer Forschung um Kennzahlen und weniger um das Technische oder Organisatorische der Informationssicherheit, sondern mehr um das Menschliche und (Unternehmens)-‚Kulturelle'. Man wollte herausfinden, wie CISOs ‚ticken'. Analysiert wurden daher Tätigkeitsfeld, Umgangsformen bzw. Behandlungsversuche vor dem Hintergrund eines tätigkeitsbezogenen Grundproblems und die Auswirkungen dieser Umgangsformen für die Wahrnehmung des CISOs und der Informationssicherheit.

Die morphologische Wirkungsforschung nutzt für Therapie wie auch für das Change-Management u.a. auch Märchen (s. a. Vergleich mit dem Froschkönig). Diese werden nicht in Hinblick auf Erzählfassung interpretiert oder durch Deutung von Symbolen. Vielmehr lassen sich im Märchen über die Auseinandersetzung mit einem Fall grundlegende Wirkverhältnisse identifizieren und in ein Bild rücken. So stellen Märchen Prototypen für die Behandlung von Wirklichkeit – gerade auch der Arbeitswirklichkeit – dar.

Medienpartner der Studie sind <kes> und securitymanager.de. Der 55-seitige Berichtsband ist (wie auch der Band der ersten qualitativen Security-Studie, »Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen«) zum Preis von Euro 380,00 über den SecuMedia-Verlag oder known_sense (sense@known-sense) erhältlich. Eine englische Version der Studie erscheint als PDF, eine Management-Summary als Beilage der <kes> – Zeitschrift für Informationssicherheit, Ausgabe 2/2008. ■

Podium nach dem Studien-Launch während der cebit am 6.3.2008: v.l.n.r. Sven Janssen (SonicWALL), Albert Schöppl (Trend Micro), Wolfgang Nickel (Steria Mummert Consulting), Norbert Luckhardt (kes), Michael Lardschneider (Münchner Rück)

Musée de Sécurité gegründet

1. Ausstellung zum Thema Awareness – auch als Roadshow unterwegs

»Schlechtes Passwort Nr. 68

»Schlechtes Passwort Nr. 99«

Am 17. Februar 2008 wurde in Köln das »Museé De Sécurité« »gegründet«. Mit diesem »Museum der Sicherheit!« möchten die Initiatoren, darunter known_sense, Informationssicherheit visualisieren und über Legenden u.a. Geschichten – Stichwörter »Storytelling« bzw. »Narratives Management« – aufbereiten, um das Thema auf unterhaltsame wie sinnliche Art erlebbar zu machen.

Die Sammlung wird auf der einen Seite »reale« Exponate präsentieren, darunter zahlreiche Awareness-Poster und -Comics, Awareness-Objekte wie z.B. den legendären »Passworthalter« und -Spiele, z.B. das Virusquartett und dessen künstlerische Illustrationen von Malware, aber auch neue Securitygames wie das Quiz »Quer durch die Sicherheit!« oder das »Hacker-Quartett« und solche, die bisher nur als Dummy bestehen und in diesem Rahmen getestet werden können.

Auf der anderen Seite werden Künstler dem Museum Redaymades zum Thema Security zur Verfügung stellen. Readymades oder das so genannte »Objet trouvé« (franz. für »gefundener Gegenstand«) sind Kunstwerke, die aus vorgefundenen Alltagsgegenständen oder Abfällen hergestellt werden, wobei Fakes (im Sinne von Behauptungen) natürlich erlaubt sind.

Ein Beispiele für die teilweise ironisch-witzige Security-Sammlung wird das Objekt »Everybody's Darling« sein, ein einfaches Vorhängeschloss, das Modell für 251 Logos oder Icons der Security-Branche war. Oder das dadaistisch anmutende Buchobjekt »The Art of Deception«, ein Umschlag des bekannten Mitnick-Titels, allerdings mit neuem Innenleben, d.h. weißen, unbedruckten Seiten.

Das Buchobjekt »Die besten schlechten Passwörter« steuert Dietmar Pokoyski bei. Es handelt sich hier um den Innenteil eines Duden mit einem neuen, dem Duden visuell angepassten Umschlag, auf dem der Titel »Die besten schlechten Passwörter« steht.

101 schlechte Passwörter

Zur Ausstellung gehören auch »101 schlechte Passwörter«, eine Objektserie mit eingravierten oder beschriebenen Texten bzw. Textfragmenten, darunter auch bekannte Wortmarken, die sich als Passwort-Memorizer ausgeben, z.B. ein Löffel mit der Gravur »Auerhahn«, etc. oder aber gefundene bzw. gefakete Zettel mit handgeschriebenen Passwörtern. Das (geheimnisvolle) Notizbuch »My Password Book« ist vollgeschrieben mit handschriftlichen Passwort-Eintragungen und wurde (angeblich) einer Psychologin im Rahmen der letzten known_sense-Sicherheitsstudie von einem Probanden präsentiert.

Und die Fotoserie »1.000 Hacker Faces« besteht aus Portraits von Personen, die Hacker mit Nachnamen heißen und in der Google-Bildsuche unter dem Schlagwort »Hacker« erscheinen.

Awareness zum Anfassen

Mit diesem innovativen Awareness-Ansatz ist das »Museé De Sécurité« Mitarbeiter-Sensibilisierung und Securitymarketing zum Begehen und Anfassen – und: Edutainment! pur. Und durch die kulturelle Aufladung des Musealen erhält sie einen ganz anderen, einen neuen wie involvierenden Stellenwert.

Die Online-Ausstellung des Sicherheitsmuseums wird im Sommer 2008 eröffnet. Die Objekte sollen aber auch als Exhibition-on-the-road auf Tour gehen und können von Unternehmen für Security-Events oder im Rahmen von Awareness-Kampagnen auf Zeit angemietet werden. ■

Online-Ausstellung ab Sommer 2008
www.musee-de-securite.de

IT-Sicherheitspreis 2007: Spielend IT-Sicherheit schaffen

Landesinitiative »secure-it.nrw« zeichnet »askit« für innovatives IT-Sicherheitskonzept aus

Mit »askit – security awareness kit«, das known_sense-Management-Tool, finden Firmen jetzt schnell heraus, warum z.B. ihren Mitarbeitern Fehlern im Umgang mit der IT oder Unternehmensdaten unterlaufen. Auf Basis von u.a. spielerischen Giveaways oder Aktionen wird Unternehmenssicherheit für die gesamte Belegschaft zu einer gemeinsamen Sache, die für mehr Involvement sorgt als »herkömmliche« Awareness-Maßnahmen. Für dieses innovative, aber bereits in der Praxis erprobte IT-Sicherheitskonzept zeichnen die Landesinitiative »secure-it.nrw« und das nordrhein-westfälische Innovationsministerium die Agentur known_sense mit dem »IT-Sicherheitspreis NRW 2007« aus.

v.l.n.r. Ankha Haucke, Dietmar Pokoyski und Udo Eichstädt

Aus welchen Gründen machen Mitarbeiter Fehler, die z.B. IT-Systeme in Unternehmen entsichern? Die Antwort klingt paradox: »Mitarbeiter wissen sehr wohl, was richtig und falsch ist«, sagt Dietmar Pokoyski, Geschäftsführer der Kölner Kommunikationsagentur known_sense, »aber je dichter das Sicherheitsnetz eines Unternehmens ist, umso mehr versuchen die Mitarbeiter unbewusst dieses System zu durchbrechen.«

Das ist das Ergebnis der von known_sense mit Partnern im Jahr 2006 durchgeführten Studie »Entsicherung am Arbeitsplatz«. Diese hat auch gezeigt, dass Mitarbeiter Unternehmenssicherheit als gemeinsame Sache erleben wollen, für die nicht nur der Securitymanager, sondern die komplette Belegschaft »kämpfen« will. »Sicherheit braucht eine Geschichte, eine verbindende Story«, beschreibt Pokoyski die Herausforderung, »das fördert den Teamgeist, die Loyalität und auch die Kreativität der Mitarbeiter.«

Auf der Grundlage der Forschungsergebnisse haben er und seine Mitarbeiter deshalb das modulare Management-Tool »askit – awareness security kit« entwickelt, mit dem Unternehmen mithilfe der Agentur Sicherheitskultur methodisch analysieren und proaktiv gestalten können. Eine psychologische Wirkungsanalyse, die u.a. intensive Tiefeninterviews und moderierte Gruppendiskussionen beinhaltet, spürt die verdeckten Motive auf, die das Verhalten der Mitarbeiter im Umgang mit IT und sensiblen Informationen beeinflussen. In der Beratung werden strukturelle Verbesserungen der Sicherheitskultur im Unternehmen entwickelt und in der Kreationsphase auf Basis zielgenauer Awareness-Maßnahmen umgesetzt.

Für dieses innovative Konzept, das IT-Sicherheit in Unternehmen qualifiziert, erhielt known_sense jetzt den »IT-Sicherheitspreis NRW 2007« in der Kategorie »Mittelstand«. Die Übergabe der Auszeichnung erfolgte am 21. November 2007 auf dem »6. IT-Sicherheitstag NRW« in Köln und belohnte die Agentur inmitten Ihrer Feldarbeit zu ihrer zweiten Securitystudie, »Aus der Abwehr in den Beichtstuhl.«.

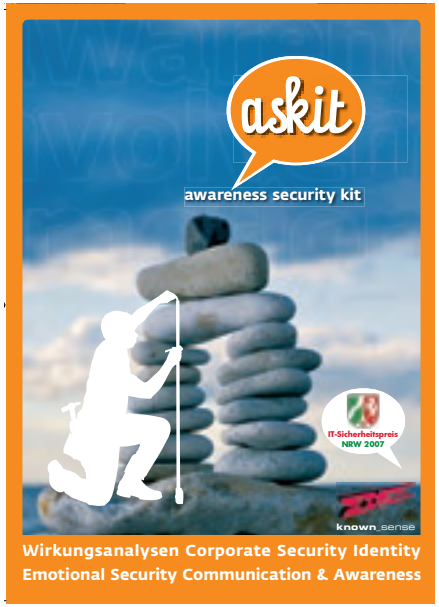
»Dieses Projekt kann andere Anwender anregen, sich mit sicherer Informationstechnik auseinanderzusetzen, und Vorbild für die Umsetzung sein«, so Thomas Faber, Leiter der Landesinitiative »secure-it.nrw«.

Der »IT-Sicherheitspreis NRW« wird seit dem Jahr 2004 verliehen. »Diese Auszeichnung ist eine hohe Anerkennung für ein Unternehmen«, betont Faber, »denn der ➔

‚IT-Sicherheitspreis NRW' hat sich in der öffentlichen Wahrnehmung zu einer Art Gütezeichen für eine sichere Firma entwikkelt.« Um den diesjährigen »IT-Sicherheitspreis NRW« haben sich zahlreiche Firmen und Schulen beworben. Eine Expertenjury ermittelte die Nominierten und Gewinner.

Infos zu den nominierten und ausgezeichneten Anwendungen enthält die Broschüre »IT-Sicherheitspreis NRW 2007 – Vorbildliche Praxis in Mittelstand und Bildung« der Landesinitiative »secure-it.nrw«. Kostenlos per E-Mail zu bestellen unter info@secure-it.nrw.de ■

Detaillierte Informationen zu askit: www.known-sense.de/askit.pdf



Wirkungsanalysen Corporate Security Identity Emotional Security Communication & Awareness

ISPIN AG und known_sense sind Awareness-Partner

Die ISPIN AG aus Bassersdorf bei Zürich, Anbieter innovative und ganzheitliche Lösungen im Bereich Informationssicherheit und Datenschutz, und known_sense haben für den Geschäftsbereich Security Awareness der ISPIN AG eine Partnerschaft vereinbart, die u.a. den exklusiven Zugriff von ISPIN auf know-how-Tranfer und Kreation der Kölner für den Schweizer Markt umfasst.

Die neue Position Architect Security Awareness bei ISPIN wird seit Januar 2008 von Marcus Beyer (32) besetzt. Bayer, Chefredakteur des Online-Fachportal Security-manager.de und auch schon einige Jahre als Trainer und Berater für Unternehmen im Bereich der internen Kommunikation, des Security Marketing und der Online-Kommunikationunters tätig, wird die die Kunden der ISPIN AG bei der Planung und Durchführung von Sensibilisierungs-Massnahmen unterstützen und in diesem Bereich auch Schulungen durchführen.

Bereits 2006 hatte Marcus Beyer gemeinsam mit known-sense den legendären »Awarenes-Koffer« mit zahlreichen außergewöhnlichen Tools für die Kunden der ISPIN kreiert. Zur Zeit startert ISPIN mit kommunikativer Unterstützung durch known_sense eine Awareness-Kampagne bei einem führenden Herstellern kardiologischer Implantate. ■

Marcus Beyer (ISPIN)

Wölfe & Geißen online – Rheinischer Security Stammtisch wird 2008 von Pallas und known_sense gesponsort

Bei WÖLFE & GEISSEN – dem 5. Rheinische Security-Stammtisch haben sich am 19. Februar 2008 in Köln erneut ca. 20 Experten versammelt, deren Tun und Wirken der Informationssicherheit und benachbarten Disziplinen verhaftet sind. Der nächste Stammtisch findet im April oder Mai 2008 statt.

Gesponsert wird das Event 2008 von Pallas und known_sense – darunter z.B. auch der begleitende Ausschank von Spitzenweinen europäischer Winzer aus dem Sortiment der Weinhandlung Ronni Hoffmann. Für 2009 sucht der Roundtable einen neuen Jahressponsor, der die Kosten für Raum, Snacks und Getränke innerhalb eines Rahmens von circa 5 Stammtischen finanziert. Bei Interesse an Sponsoring oder einer Einladung wenden Sie sich bitte an sense@known-sense.de ■

www.woelfegeissen.de

known_sense-Akteure live als Speaker:

02.04.2008 Berlin (Bitkom) D. Pokoyski
22.04.2008 Zürich (Brasserie Lipp/ISSS) D. Pokoyski
03.06.2008 Bad Homburg (SECURE) A. Haucke

Olé Nr. 9 erscheint im Juni 2008.

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