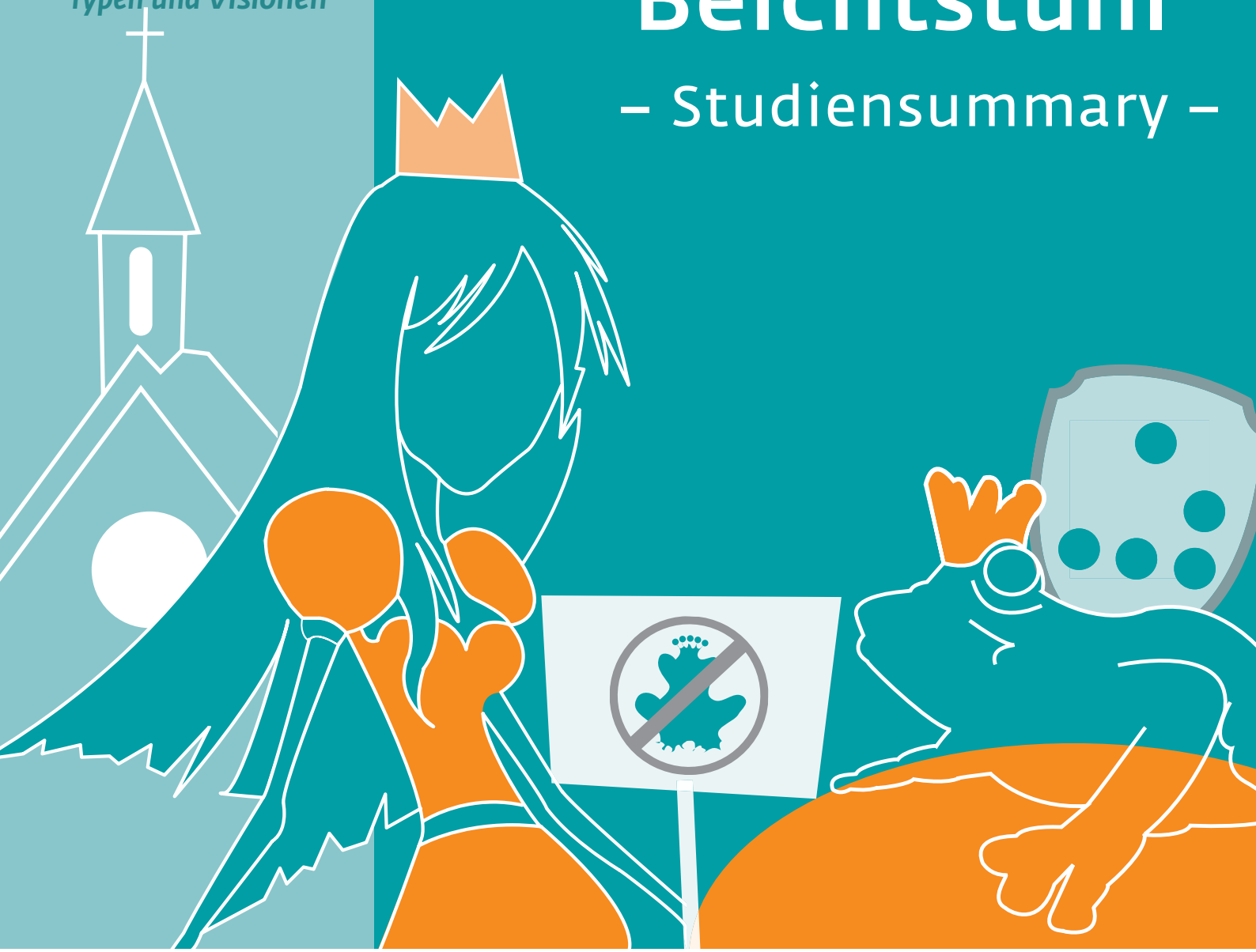
Tiefenpsychologische Security-Studie 2008:

Die Wirklichkeit von CISOs – Strategien, Typen und Visionen

Aus der Abwehr in den Beichtstuhl

– Studiensummary –



Qualitative Wirkungsanalyse CISO & Co.

Medienpartner

<kes> Die Zeitschrift für Informations-Sicherheit

securitymanager.de Das IT-Security Portal

Eine tiefenpsychologische Studie von

EnBW known_sense pallas SAP SONICWALL steria mummert consulting TREND MICRO Securing Your Web World

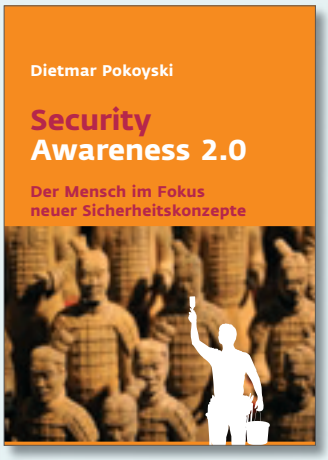
Forschung

Aus der Abwehr in den Beicht-stuhl – qualitative Wirkungs-analyse CISO & Co.
Köln, 2008. 55 S. € 380,00 (Print dt., PDF dt./engl.)
Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen.
Köln, 2006. 64 S. € 380,00 (Print dt., PDF dt./engl.)
Beide Studien im Bundle € 480,00

Methodik & Tools

askit – awareness security kit.
Hier erfahren Sie mehr über die Methodik der Security-Wirkungs-analyse und über unsere Aware-ness-Kampagnen und -Tools. Für einen besonders vorbildlichen Beitrag zur Informationssicherheit ausgezeichnet mit dem IT-Sicher-heitspreis NRW 2007.
www.known-sense.de/askit.pdf

Essays & Praxis



Security Awareness 2.0. Der Mensch im Fokus neuer Sicherheitskonzepte.
Wie identifiziere ich Sicher-heitskultur? Was bedeutet eigentlich AWARENESS? 132 S. E-Book. Verfügbar ab 07/2008
www.known-sense.de

known_sense

Impressum *Erschienen als Beilage der <kes> N. 2 (2008)*

Herausgeber der Studie
EnBW Energie Baden-Württemberg AG, known_sense, Pallas GmbH, SAP AG, SonicWALL Deutschland, Steria Mummert Consulting AG, TREND MICRO Deutschland GmbH

Medienpartner der Studie
<kes> – Die Zeitschrift für Informationssicherheit
securitymanager.de

Wirkungsanalyse
Dipl. Psychologe Udo Eichstädt (Projektltg.)
Dipl. Psychologin Ankha Haucke (Projektltg.)
Dipl. Psychologe Andreas Pieper

Feldorganisation
K & M Forum, Köln, known_sense

Gestaltung (Studie & Summary)
Carina Linnemann, Dietmar Pokoyski (known_sense)

Konzept, Produktion Studie/Herausgeber Summary
known_sense
Kaiser-Wilhelm-Ring 30-32 / D-50672 Köln
Fon +49 221 91277778 / Fax +49 221 2403910
sense@known-sense.de / www.known-sense.de

Hintergrund dieser Studie

Im Sommer 2006 beauftragte die Kommunikationsagentur known_sense ein Team von Psychologen mit einer Grundlagenforschung zum Thema Information Security. Auf Basis der Morphologischen Markt- und Medienforschung sollten in einer tiefenpsychologischen Studie die Faktoren ermittelt werden, die für die oft zitierten Fehlleistungen von Mitarbeitern verantwortlich sind.

Partner waren <kes>, der Deutsche Sparkassen Verlag, die EnBW Energie Baden-Württemberg AG, nextsolutions, die Pallas GmbH und – für die englische Übersetzung – Hewlett Packard. Im Oktober 2006 wurde der 64seitige deutschsprachige Berichtsband »Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen« im Rahmen einer Pressekonferenz auf der Münchener SYSTEMS vorgestellt.

Das große Interesse an dieser Grundlagenstudie, deren Ergebnisse auf S. 11 zusammengefasst sind und deren Weiterentwicklung u.a. auch durch die Auszeichnung mit dem IT-Sicherheitspreis NRW 2007 (für »askit – awareness security kit«) betont wurde, verstanden die Initiatoren als Aufforderung, auch die Einzelteile der Information Security (tiefenpsychologisch) näher zu analysieren. Die hier vorliegende Studie bildet nun Teil I einer Reihe weiterer geplanter Untersuchungen dieser Teilaspekte; in Vorbereitung sind u.a. Studien zum Thema Mobile Security und zur Sicherheitskultur in Europa, ausgehend von einem interkulturellen D-A-CH-Vergleich. *

Die vorliegende aktuelle Wirkungsanalyse widmet sich aber in logischer Konsequenz denjenigen, die der in der Grundlagenstudie zu Wort kommenden Gruppe (den Usern bzw. Mitarbeitern) diametral gegenüberstehen: den Sicherheitsverantwortlichen in den Unternehmen (nachfolgend der Einfachheit halber stets CISO – Chief Information Security Officer – genannt). Bereits im Rahmen der Grundlagenstudie wurde deutlich, dass gerade diejenigen, die die Entsicherungen bewusst verhindern sollen, ebenfalls in einem Dilemma stecken: Einerseits begegnen ihnen Mitarbeiter durchaus ambivalent, andererseits ist den CISOs selbst eine sowohl sichernde als auch entsichernde Seite inhärent (s. Entsicherung am Arbeitsplatz, S. 43). Dieses Dilemma wird u.a. in der aktuellen Studie ausführlich und auf den folgenden Seiten im Rahmen einer Summary des 55-seitigen Berichtsbandes beschrieben.

Köln, im Mai 2008

** Auf Anregung von Studienpartnern soll in Kürze zudem eine Fortsetzung dieser Forschung in Form einer CISO-Image-Analyse inklusive Mapping mit den hiesigen Ergebnissen produziert werden, bei der Management u.a Entscheider zu Ihrem Bild von CISOs/Sicherheitsverantwortlichen befragt werden.*

»Die Bedeutung der IT-Sicherheit für das Geschäft steigt mit der Bedeutung der IT. Um ein angemessenes Sicherheitsniveau für das jeweilige Geschäft zu erreichen, ist eine ganzheitliche Betrachtung erforderlich. Auch das Bewusstsein auf Geschäftsseite ist zu verbessern. Dabei stehen die CISOs mit ihrer Aufgabe immer im Spannungsfeld zwischen Effektivität, Effizienz und Sicherheit. Sie moderieren den Security-Prozess. Moderieren heißt »dienen«, was einen ständigen Spagat bedeutet. Loyalität gegenüber dem Unternehmen steht dabei im Vordergrund. Einhaltung, Kontrolle und Schaffung von Bewusstsein sind Erfolgsfaktoren für IT-Sicherheit. Die Studie ist ein wertvoller Beitrag, damit die Prozesse im Security-Management und darüber auch die CISOs nicht »entmenschlicht« werden. Die CISOs müssen eine »Marke« werden. Dann werden sie Erfolg haben – auch ohne »jedermanns Liebling« sein zu müssen. Denn wenn der CISO der beliebteste Mann im Unternehmen ist, macht er etwas falsch!«

Wolfgang Reibenspies, Konzernbevollmächtigter IuK-Security EnBW Energie Baden-Württemberg AG

Die Wirklichkeit als CISO

Selbstbild, Image, Wirkung und Visionen – neue tiefenpsychologische Studie nimmt Sicherheitsverantwortliche unter die Lupe

»Woher komme ich? Was bin ich? Wo gehe ich hin? Mehr noch: Auf welche Weise? Auf welchen Wegen? Und vor allem: Wie geht es weiter mit meinem Beruf, in meinem Unternehmen?« Die im März 2008 von der EnBW, known_sense, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro Deutschland 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 Officer) 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 und z.B. davon ab, 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. D.h. ein Teil der angefragten CISOs war bereit und interessiert, an einem Gespräch über sich und ihr Berufsleben teilzunehmen. Ein anderer Teil beendete die Anfrage abrupt. In einigen Fällen gestaltete sich die Kontaktphase als ein langwieriger Vor- und-Zurück-Prozess (indem beispielsweise eine anscheinend klare Absage erteilt wurde, man aber dennoch neugierig in der Leitung blieb, ohne das Gespräch zu beenden).

> *„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.*

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 Inter-

Zahlen und Fakten

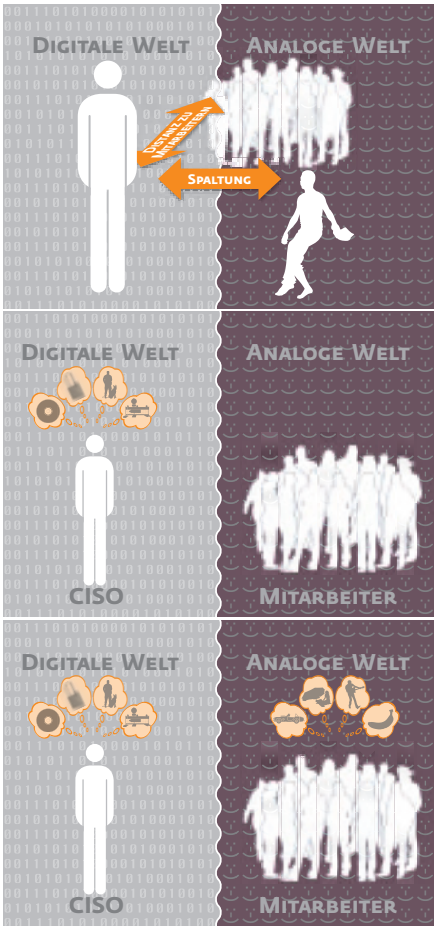
Für die Studie »Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co.« wurden insgesamt 30 Sicherheitsverantwortliche aus Nordrhein-Westfalen in einem Studio in Köln oder innerhalb von Office-Interviews on Location mithilfe morphologischer Markt- und Medienforschung (s. Methodik S. 9) befragt. Das Dienstalter der Probanden betrug 2-5 Jahre, 6-10 Jahre und mehr 10 Jahre (paritätisch). Alle 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 (11 mittelständische Unternehmen mit durchschnittlich 500 Mitarbeitern und 19 Großunternehmen mit durchschnittlich 30.000 Mitarbeitern, gerundeter Durchschnitt aller Firmen: 20.000 Mitarbeiter).

Ziel der von EnBW, known_sense, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro Deutschland

view 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.

Die Form der zwischen-menschlichen Beziehung wird zu einem zentralen Thema – sowohl innerhalb der Interviews als auch in der Beschreibung der konkreten Arbeit der CISOs. Mal wird in den Interviews relativ schnell eine große Nähe hergestellt. Ein anderes Mal herrscht eine scheinbar unüberbrückbare Distanz zwischen den Beteiligten. Die Begegnungen mit den CISOs erinnern oftmals an das Erleben im Umgang mit einem Kippbild (optische Illusion). Es entsteht der Eindruck, die CISOs seien hin- und hergerissen. Mal gerät man in einen regen Austausch mit ihnen, dann wiederum hat man den Eindruck, wie vor verschlossenen Türen zu stehen. Die verschiedenen Haltungen führen keine Beziehung untereinander. Sie wirken wie getrennt. In diesem Sinne ist die Psycho-Dynamik dieser Studie durch eine Tendenz zur Spaltung gekennzeichnet – einem Mal-so-mal-so.

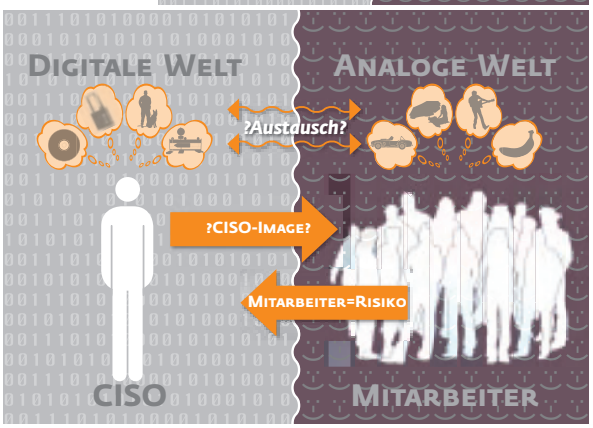
> *Selbst die Putzfrau trägt dazu mehr bei, indem sie dafür sorgt, dass das Gebäude nicht schmutzig ist und die Kunden sich wohl fühlen.*



Ein zufälliges Hineingeraten…

Die berufliche Entwicklung hin zur Position des CISOs wird von den Befragten als eine eher zufällige Entwicklung dargestellt. Die Ausbildungen und Berufsentwicklungen der Befragten waren in der Regel nicht auf eine Tätigkeit als CISO ausgerichtet. Die Befragten hatten die Tätigkeit des CISOs ursprünglich nicht auf ihrem Berufswunschzettel. Bei Ausscheiden des vorherigen CISOs wurde man gefragt, »ob man das nicht machen will(?).«

Die Anfrage an den Mitarbeiter, CISO im Unternehmen zu werden, wird von den Befragten ambivalent aufgenommen. Einerseits wird es als Auszeichnung empfunden, mit dieser verantwortungsvollen Tätigkeit betraut zu werden. Andererseits entsteht der Eindruck, dass es in erster Linie darum geht, diesen Bereich möglichst reibungslos zu besetzen.Die CISOs selber schwanken in der Wertschätzung ih-



verantworteten Forschung war die Darstellung und Erforschung des CISO-Berufsbilds, wobei hierunter auch 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 um das Menschliche und (Unternehmens)-Kulturelle. Man wollte also herausfinden, wie CISOs wirken und mit welchen Strategien – kurzum: wie sie ticken. Analysiert wurden daher Tätigkeitsfelder, Umgangsformen bzw. Behandlungsversuche vor dem Hintergrund eines tätigkeitsbezogenen Grundproblems und die Auswirkungen dieser Umgangsformen für die Wahrnehmung des CISOs und der Informationssicherheit. Formale Strategien technischer und organisatorischer Sicherheit wurden aus Gründen der Interview-Qualitätssicherung nicht explizit abgefragt, sind aber als Teil der in der Studie beschriebenen Behandlungsversuche in den Ergebnissen integriert.

Der 55-seitige. Berichtsband ist zum Preis von € 380,00 über den SecuMedia-Buchshop oder via sense@known-sense.de erhältlich (für <kes>-Abonnenten Sonderpreis € 290,00). Eine englische Version der Studie existiert in PDF-Form.

rer eigenen Tätigkeit. Die Möglichkeit, direkt etwas zu werden, siegt allerdings über das Abwägen eines Für und Wider dieser Tätigkeit. So bestimmen von Beginn an sowohl Besonderes als auch Banales die Wahrnehmung dieser Position.

Als eine 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.

> *„Ich bin die ärmste Sau im Betrieb. Freunde habe ich da nicht.“*

Leiden im Untergrund

Eine solche 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.

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, 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.

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, dass 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

CISO-Typen: Von Fräulein Rottenmeier über Mutter Teresa bis hin zu Columbo

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,

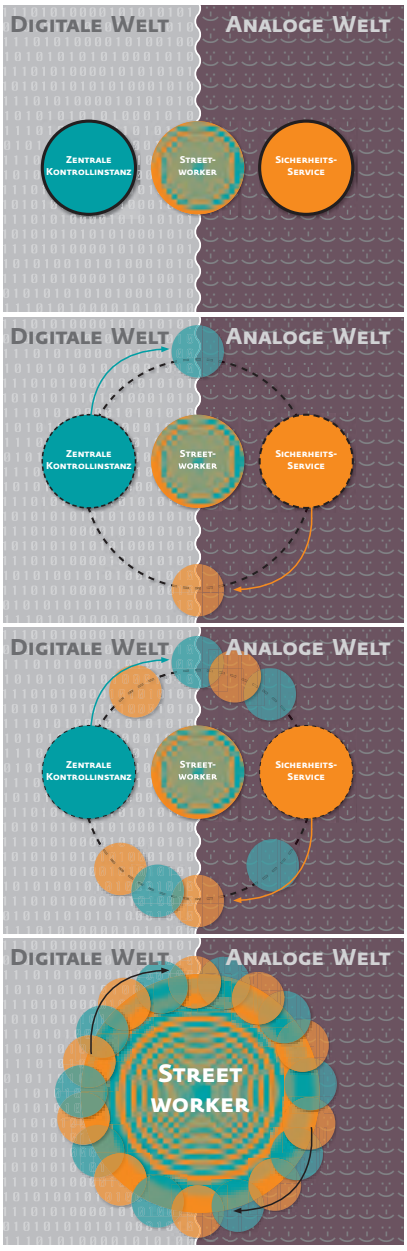
schafft er es oftmals nicht, die Relevanz seiner Belange durchzusetzen. So fürchtet er letztlich doch um seine Existenz im Unternehmen, z.B. durch die vermeintliche Bedrohung durch externe Security-Sevice-Anbieter. »Ich komme mir vor wie ein Mann vom ADAC. Den holt man auch nur, wenn man am Strassenrand liegen geblieben ist«, sagt einer, 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 = 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 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 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.

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. Er entsichert sich selbst, um der analogen Sichtweise der Mitarbeiter zu begegnen. Diese Strategie setzt – anders als die die beiden anderen – nicht auf Spaltung, sondern auf ein Verzahnen der beiden unterschiedlichen Prinzipien.



Märchenanalyse: Prinzessin, Frosch oder beide

Am Ende 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 (s. a. Märchenanalyse im Kasten Methodik auf S. 9). 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.« Es entwickelt sich ein Ringen um Positionen. Dabei kommen sich beide Formen – das froschhafte Banale und die prinzessinhaften entwickelten Züge – immer näher. Die Entwicklung wird eben in jener Situation fortgesetzt, in der sich die Prinzessin in Entschiedenes, Gemeines wandelt (wiederentdeckt) und den Frosch an die Wand wirft, der sich nach dem Wurf in einen Prinzen verwandelt. Damit geraten beide (ehemals) getrennte Formen wieder in Zirkulation.

Die Strategien Zentrale Kontrollinstanz und Sicherheits-Service betonen die Trennung von Prinzessin und Frosch. Hierin wird die paradoxe Einsicht vermieden, dass sich Froschiges in Prinzesinnenhaftes wandeln kann und umgekehrt. Ebenso wird der Erfahrung aus dem Weg gegangen, dass Sicherheit nur durch das Einlassen auf Risiken lebbar und produktiv bleibt. Eine Figur, die dieses Ineinander verkörpert, ist z.B. Peter Falk als Columbo. Er entspricht am ehesten dem Typus Streetworker.

»Die Studie zeigt, dass das Verhalten der CISOs nicht nur rational, sondern auch durch emotionale Impulse bestimmt wird. 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.«

Wolfgang Nickel, Senior Manager Competence Center IT-Security Steria Mummert Consulting AG

Im Bild des Eisernen Heinrich und der brechenden eisernen Bande verdeutlicht sich laut Studie sowohl das Eingezwängtsein als auch das Öffnende der jeweiligen Strategien. Die Typen Zentrale Kontrollinstanz und Sicherheits-Service haben eben jene Verschlossenheit im Interview spürbar werden lassen. Zugleich war aber auch stets erfahrbar, dass eine Verwandlung, ein Einbeziehen des Getrennt-Gehaltenen zu einer Öffnung und Befreiung führte (Streetworker). Dem Märchen gelingt es, ein Gespür für das jeweils Fehlende zu erzeugen.

Nicht in eiserne Bande einzwängen

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.

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, 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.«

Fazit

Der CISO ist mit einer paradoxen Anforderung konfrontiert. Er spürt, dass er ein Sicherheitsrisiko eingehen muss, um für eine stabilere Sicherheitskultur zu sorgen. Zugespitzt kann man sagen: Entsicherung produziert Sicherheit – der CISO muss nun entscheiden, an welcher Stelle Entsicherungen vertretbar sind! Die pragmatische Formel: »100% Sicherheit gibt es nicht, 80% sind ausreichend« stellt aus dieser Perspektive eher eine Belastung als eine Erleichterung dar. Es ist einfacher, sich an dem Versuch einer 100%igen Sicherheit abzuarbeiten als sich auf ein Ineinander von Sicherheit und Gefährdung, von analogem und digitalem Prinzip einzulassen.

Aus Sicht des Streetworkers (Columbo) passt das. Er schafft es, 20% Risiko einzusetzen und gemeinsam mit den Mitarbeitern zu verantworten. Die Zentrale Kontrollinstanz (Fräulein Rottenmeier) will keine 20%ige Risikobelastung, sondern ein unbeschwertes Dasein. Der Sicherheits-Service (Mutter Teresa) trägt bereits mehr als 20% Risiko. Hier geht es eher darum, 80% Sicherheit zu erreichen. ■

»Aus der Studie habe ich gelernt, dass die Informationssicherheit auf drei Beinen steht: Technik, Organisation und Unternehmenskultur. Gerade die kulturelle Komponente prägt dabei das Wirken des CISOs. Mich beschäftigt nun, wie ich den CISO dabei unterstützen kann, seine Wirksamkeit wahrnehmbar zu machen. Dazu liefert die Studie eine ordentliche Menge Stoff.«

Dr. Kurt Brand, Geschäftsführer der Pallas GmbH

Methodik der Studie

Auf der Grundlage der morphologischen Psychologie, die an der Universität Köln entwickelt wurde, analysieren erfahrene Psychologen und Markt- bzw. Medienforscher mithilfe des von known_sense entwickelten und mit dem IT-Sicherheitspreis NRW 2007 ausgezeichneten Tools »askit – awareness security kit« die unbewussten seelischen Einflussfaktoren und Sinnzusammenhänge von IT und Information Security. Vorgenommen werden die Analysen in der Regel auf der Basis von Tiefeninterviews.

Beim psychologischen Tiefeninterview wird so tief gegraben, bis die Interviewer in der Lage sind, die psychologische Wurzel eines Phänomens erkennen und beschreiben zu können. In den zweistündigen Einzelinterviews decken sie die unbewussten seelischen Wirkungen und Einflussfaktoren auf, die das Verhalten aller von der Security betroffenen Personen bestimmen. Diese werden motiviert, in ihrer eigenen Sprache alles zu beschreiben, was ihnen im Zusammenhang mit Ihrer Arbeit, ihrem Wirken und der Unternehmenssicherheit durch Kopf und Bauch geht. So sind diese Explorationen gewissermaßen Forschungsreisen, auf denen Probanden und Interviewer bisher unverstandene Phänomene gemeinsam erkunden. Dabei werden die geheimen bzw. nicht bewusst wahrgenommenen Bedeutungs-Zusammenhänge erforscht und nachvollziehbar gemacht. D.h. in einem derartigen Setting eröffnen sich stets neue Wendungen und oft überraschende Einblicke, die dann systematisch auf ihre Verhaltensrelevanz weiterverfolgt werden.

Der Vorteil dieser Methode: Es werden alle verdeckten Motive erfasst und in einen PSYCHO-LOGISCHEN Kontext gestellt. Auf Basis dieser Ergebnisse können dann zielgenaue und konkrete Empfehlungen zur Verbesserung der Sicherheitskultur eines jeden Unternehmens formuliert werden.

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.

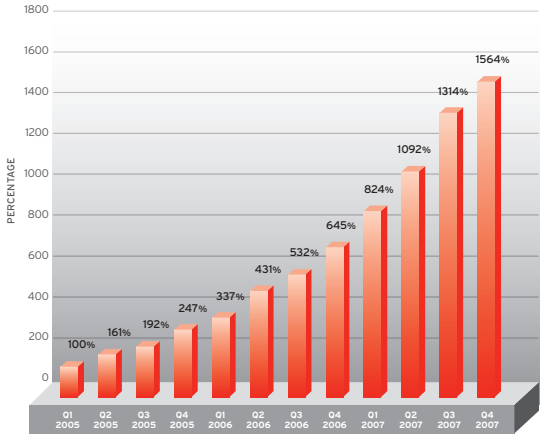
www.known-sense.de/askit.pdf

Sicherer Datenverkehr in beide Richtungen

Es ist ein Kreuzfeuer aus internen und externen Bedrohungen, dem Unternehmen heute ausgesetzt sind. Um inmitten des Kräftefeldes aus Gefahren, Regularien und Effizienzdruck einen reibungslosen und sicheren Informationsfluss zu gewährleisten, stehen besonders Sicherheitsverantwortliche vor zwei drängenden Herausforderungen: Einerseits nutzt die professionelle und finanziell motivierte Malware-Szene ein wachsendes Arsenal von Web Threats, um die Sicherheitslösungen am Perimeter zu umgehen und Trojaner, Spyware, Keylogger etc. einzuschleusen. Andererseits verlassen Geschäftsdokumente unbemerkt das Unternehmen, weil durch Unkenntnis oder Absicht interne Datenlecks geöffnet werden. Umfassende Sicherheit ist nur durch eine präventive Strategie zu erreichen, die sowohl interne als auch externe Bedrohungen berücksichtigt. Sicherheitsverantwortliche benötigen aus diesem Grund zuverlässige Lösungen, mit welchen sie die Datenströme am Perimeter und im Internet wie auch im Unternehmen regeln können.

Verkehrsüberwachung am Datenhighway

Während Script-Kiddies noch vor wenigen Jahren mit globalen Virenangriffen zu fragwürdigem Ruhm gelangten, sind die Absichten heutiger Cyberkriminellen weniger ideell: Hoch professionelle und finanziell motivierte Hackerbanden prägen eine neue Bedrohungslandschaft. Rund um die Erstellung, den Verkauf und den Einsatz von Malware ist ein regelrechtes Wirtschaftssystem entstanden. Ein Indiz für die Attraktivität der betrügerischen Geschäftsmodelle ist die Zunahme von Web Threats um 1564 % zwischen 2005 und 2007.



Quelle: Trend Micro

Demzufolge bilden Web-basierte Angriffe die größte Bedrohung für die Sicherheit von Unternehmen. Alleine der Besuch einer Webseite reicht aus, eine komplexe Infektionskette im Hintergrund zu starten und seinen Rechner unbemerkt zu infizieren. Auch viele an sich seriöse Web-Angebote sind gehackt bzw. kompromittiert, wodurch die Begrenzung auf »gute« Seiten keine Sicherheitsgarantie mehr verspricht.

Ist ein Rechner infiziert, werden im Regelfall weitere schadhafte Komponenten dynamisch nachgeladen. Die eingesetzten Infektionstechniken sind flexibel und vielfältig, die Ziele einfach: Diebstahl vertraulicher Daten und Aufbau von Bot-Netzen für die kommerzielle Nutzung. Auf Basis des herkömmlichen Zyklus aus Malware-Erkennung sowie Pattern-Generierung und -Verteilung können Web Threats nicht effizient bekämpft werden. Trend Micro hat diese Entwicklung frühzeitig erkannt und mit der Web Threat Protection eine Technologie entwickelt, die Informationen aus verschiedenen Datenquellen wie Web- und E-Mail-Reputation sowie Botnet-Identifikation kombiniert. So werden Anwender bei der Internet-Nutzung in Echtzeit geschützt. Diese Erweiterung des lokalen Antiviren-Schutzes durch Sicherheitsmaßnahmen im Internet blockiert gefährliche Daten bereits vor dem Internet-Gateway.

Riskante Datenmanöver

Wesentliche Aufgabe der IT-Sicherheitsverantwortlichen ist – neben der Abwehr von externen Angriffen durch Hacker und Malware – die Sicherstellung der Verfügbarkeit, Unversehrtheit und Vertraulichkeit der im Unternehmen gespeicherten Informationen. Verlassen kritische Daten unbemerkt das Unternehmen, gehören Imageschäden und negative Schlagzeilen noch zu den harmlosen Folgen. Nach geltendem Recht gehört die Gewährleistung der IT-Security zu den Pflichten der Geschäftsleitung – durch Vorschriften wie Basel II, § 8 VOL/A und Sarbanes-Oxley drohen bei Nichtbeachtung zivilrechtliche Schadensersatzansprüche von Geschädigten gegen das Unternehmen.

Reisepass für Dokumente

Mit LeakProof 3.0 bietet Trend Micro eine Lösung, die kritische Daten im Speicher, bei der Bearbeitung und während der Übertragung schützt. Die Lösung erstellt für jedes Dokument einen einzigartigen Fingerabdruck, der die lückenlose Verbreitungskontrolle

und Nachverfolgung ermöglicht. So wird verhindert, dass sensible Informationen über Netzwerkkanäle oder Datenträger wie USB-Sticks und CDs/DVDs aus dem Unternehmen gelangen. Durch interaktive Warnmeldungen stärkt LeakProof 3.0 darüber hinaus das Risikobewusstsein der Mitarbeiter und fördert den verantwortungsvollen Umgang mit Unternehmensdaten. Dieser Ansatz unterscheidet die Trend Micro Lösung deutlich von anderen Anbietern, da der »Sicherheitsfaktor Mensch« bewusst in die Sicherheitskultur eines Unternehmens eingebunden wird. Über Mitarbeiteraufklärung werden Vorgänge schon im Vorfeld verhindert, die zu Datenverlust führen können. ■

Rückblick: Die Pilotstudie »Entsicherung am Arbeitsplatz« (2006)

Im Rahmen der Grundlagenstudie »Entsicherung am Arbeitsplatz« hatte das für die aktuelle Studie »Aus der Abwehr in den Beichtstuhl« verantwortliche Psychologen-Team bereits im Sommer 2006 ebenfalls auf Basis morphologischer Wirkungsforschung Angestellte nach ihren Gewohnheiten und Wünschen im Umgang mit IT-gestützter Arbeit und nach ihren Vorstellungen von und Erfahrungen mit IT-Security und Unternehmenskultur befragt.

Die Ergebnisse in Kürze: Wird die Schutzfunktion von Information Security auch als positiv und notwendig erachtet, so verkehrt sich dieser Schutz nicht selten in ein Zwangsystem, das Identität und individuelle Gestaltungswünsche der Mitarbeiter ausschließt. Der Umgang mit Information Security und ihr unmittelbares Erleben werden zu einer Frage des Vertrauens in das Unternehmen und sind so untrennbar mit dessen Selbstverständnis verbunden. Nur wenige Unternehmenskulturen erlauben Raum für Eigenes; Arbeit, insbesondere Computerarbeit, versachlicht sich – speziell durch den geforderten Umgang mit IT-Security. Entsicherndes Handeln wird zum unbewussten Befreiungsschlag gegen das Unternehmen im Allgemeinen und die IT wie Information Security im Besonderen. Die Studie macht deutlich: Je weniger Raum für Eigenes vorhanden ist, umso mehr besteht die Gefahr einer Verkehrung und damit des unkontrollierten Ausbruchs entsichernder Handlungen.

Dabei verkehrt sich das Phänomen des Sachlichen Verschliessens (Schutz vor Ein- und Ausbrechern) in Ausbrüche, die dem Prinzip des Menschlichen Eröffnens folgen: Mitarbeiter machen mithin unbewusst Fehler, um so ihre überwiegend digitale und damit weitgehend bildlose und entpersonalisierte Arbeit wieder menschlicher zu gestalten und damit ihre persönliche Produktivität zu sichern. Die Studie kommt zu der Erkenntnis: Je weniger Raum für Eigenes vorhanden ist, umso eher besteht bei den Mitarbeitern die Gefahr einer Verkehrung und damit des unkontrollierten Ausbruchs entsichernder Handlungen. Bei Mitarbeitern, die die zunehmende Entmenschlichung von Arbeit nicht länger aushalten, kommt es zu den oftmals zitierten Fehlern, bei denen die Mitarbeiter ihr Unternehmen entsichern. Das Fazit: Die Mehrheit so genannter Fehlleistungen stellen an sich – also in der Logik der Mitarbeiter – etwas Positives dar, mit dem aktiv, aber unbewusst Selbsterhalt betrieben wird.

www.known-sense.de/entsicherung/securitystudie_pr_launch.pdf

»Woher komme ich? Was bin ich? Wo gehe ich hin? Und vor allem: Auf welche Weise? Auf welchen Wegen? – Wie geht es weiter mit meinem Beruf – in meinem Unternehmen?« – Die entscheidenden Fragen, die sich Sicherheitsverantwortliche stellen, unterscheiden sich auf den ersten Blick nicht weiter von den klassischen, existenziellen Fragen anderer Berufstätiger. Und dennoch steckt im Detail das grosse Besondere, das gerade CISOs so unverwechselbar macht.

In dem Berichtsband, der der hier vorliegenden Studiensummary zugrunde liegt, begegnen wir verschlossenen Haltungen mit unverrückbaren Positionen und wortkargen Darstellungen – einem Leiden im digitalen Untergrund. Einem ständigen Ringen mit sich und den Mitarbeitern, die dem analogem prinzip verhaftet sind und die einen von heute auf morgen als einen Anderen betrachten, wenn man (scheinbar ohne großes persönliches Zutun) in die jetzige Position gerät. Einem Wechsel in eine doch seltsame Zwischenwelt, der – wenn er nicht gelingt – vielen wie verhext erscheint und nicht selten zu Spaltungen und Identitätskrisen des CISOs führt.

Andererseits wird auch ein ausgesprochenes Mitteilungs- und Verstehensbedürfnis der CISOs spürbar. Man ringt um den grossen Auftritt, in dessen Rahmen man sich ab und zu eine Würdigung erhofft. Nur wie, wenn man stets das Gefühl hat, dass man selbst kaum Konkretes produziert – etwas, das man an die Wand hängen oder vorzeigen kann? Etwas, an dem man die eigene Wirksamkeit erleben und demonstrieren darf.

Nach Entsicherung am Arbeitsplatz geht es hier erneut um den Menschlichen Faktor der Sicherheit. Und wie in der Studie von 2006, die eine (psychologische) Auflösung der Wirkprinzipien so genannter Mitarbeiter-Fehlleistungen präsentiert, werden in dieser zweiten qualitativen Securitystudie erneut Einzelteile der Informationssicherheit auseinander genommen, unter der (tiefenpsychologischen) Lupe betrachtet und wieder zusammengeschraubt, bis die Problemzonen in Drehung geraten. Dadurch werden ehemals verschüttete, geheime Faktoren an die Oberfläche der Information Security befördert, und es entsteht ein (überschaubares) Ganzes, mit dessen Hilfe Wirkungen beschrieben und Learnings für alle Protagonisten und Zielgruppen von Sicherheit abgeleitet werden können.