Abwehrchef oder Beichtvater?!

Psychologische Studie zu Wirken und Visionen von CISO & Co.

Verantwortliche für IT-Sicherheit haben noch kein klares, eingefahrenes Berufsbild; dementsprechend unscharf sind bisweilen sowohl eigene als auch äußere Erwartungen an „CISO & Co." Eine psychologische Studie ist Eigen- und Fremdbild der CISOs nachgegangen – erste Vorab-Ergebnisse gibt es hier exklusiv für <kes>-Leser.

Von Dietmar Pokoyski, Köln

„Was? Es interessiert sich jemand für unseren Beruf?" – so oder ähnlich überrascht bis ungläubig reagierten viele IT-Sicherheitsverantwortliche beim Zusammentreffen mit Psychologen der Kölner Agentur known_sense im vergangenen Winter. Für die Studie „Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co." wurden insgesamt 30 Sicherheitsverantwortliche aus nordrhein-westfälischen Unternehmen zwischen 50 und 110000 Mitarbeitern in zweistündigen Interviews befragt. Ziel war die Untersuchung des CISO-Berufsbilds, wobei hierunter jegliche leitenden IT-Sicherheitsbeauftragte und verwandte Berufsvertreter zu verstehen sein mögen.

Auf Basis morphologischer Markt- und Medienforschung hatte dasselbe Team bereits im Sommer 2006 Angestellte nach ihren Gewohnheiten und Wünschen im Umgang mit IT-gestützter Arbeit und nach ihren Vorstellungen von IT-Security und Unternehmenskultur befragt (vgl. <kes> 2006#6, S. 61). Ein wichtiges Ergebnis war, dass Mitarbeiter unbewusst „Fehler" machen, um so ihre „entpersonifizierte" IT-Arbeit wieder menschlicher zu gestalten und damit ihre persönliche Produktivität zu sichern. Die Studie betrachtete Sicherheit dabei stets auch im Kontext von Unternehmenskultur und hat verdeutlicht: Je weniger Raum für Eigenes vorhanden ist, umso eher besteht bei den Mitarbeitern die Gefahr einer Verkehrung und damit des unkontrollierten Ausbruchs „entsichernder" Handlungen.

Menschliches und (Unternehmens)-„Kulturelles" stand auch im Mittelpunkt der neuen Studie, die nunmehr Erkenntnisse zum Leben und Wirken der CISOs liefern soll. Denn auch das zumeist äußerst sachlich angegangene Thema der Informationssicherheit zeigt in der (teils mangelnden) Kooperation mit Kollegen sehr viele allzu menschliche Züge: etwa, wenn ein CISO berichtet, den Mitarbeitern aus der Unternehmenskommunikation erstmal eine ganze Reihe Cappuccinos ausgeben zu müssen, bevor bei Awarenessmaßnahmen überhaupt an eine Kooperation zu denken ist.

Ziele

Die aktuelle Wirkungsanalyse zu CISO & Co. planen ihre Urheber als Start einer ganzen Reihe von Studien zum Themenkomplex „Sicherheitskultur in Europa". Speziell mit der CISO-Forschung soll ein besseres Verständnis dieses strategisch wichtigen, aber relativ jungen, „geschichtslosen" und nicht zuletzt komplexen Berufstands ermöglichen. Inhaltlicher Kern werden eine Image- und Positionierungsanalyse sowie die Erstellung einer Typologie sein, aus der Erkenntnisse für sämtliche Zielgruppen zu erwarten sind, die im Kontext von Informationssicherheit agieren:

_____ Sicherheitsbeauftragte sollen über die Studie einen aufschlussreichen Selbstbild/Fremdbild-Abgleich sowie eine fundierte Analyse der Stärken und Schwächen erhalten, aus denen sie Rückschlüsse auf sich, ihre Arbeit und die Sicherheitskultur in ihrem Unternehmen sowie ihre exakte Positionierung gegenüber Vorgesetzten, IT-Abteilung, Unternehmenskommunikation, Mitarbeitern et cetera ableiten können.

_____ Unternehmen und ihre Security-Consultants sollen bisher weitgehend „verschüttete" psychologische Erkenntnisse bezüglich der aktuellen Sicherheitskultur sowie über den Zusammenhang von Sicherheitskultur und Auftritt sowie Positionierung ihrer CISOs erhalten.

_____ IT- und Kommunikationsabteilungen sollen Anregungen und Handlungsempfehlungen zur Optimierung der internen Kommunikation erhalten, vor allem bezüglich der Kommunikation mit dem IT-Sicherheitsbeauftragten.

_____ Entscheider und Personalmanager sollen klassifizierte Kriterien zur Beurteilung von CISO-Profilen erhalten.

Für Security-Dienstleister und Fachmedien soll die Studie fundierte Informationen über ihre Zielgruppe liefern und eine produktive Ansprache von IT-Sicherheitsbeauftragten sowie IT-Abteilung fördern.

Kommunikationsagenturen und Awareness-Dienstleister sollen aus den Studienergebnissen Coachings, Kommunikationsbriefings und andere „weiche" Tools für IT-Sicherheitsbeauftragte entwickeln können, welche die eingangs skizzierten Bedingungen und die spezielle Situation der CISOs berücksichtigen.

Erkenntnisse

Zum Redaktionsschluss der vorliegenden <kes> war die Gutachtenerstellung noch nicht abgeschlossen; aus der laufenden Analyse konnten die Psychologen aber bereits einige Phänomene beschreiben: „Zunächst fällt auf", berichtet die Projektleiterin Diplom-Psychologin Ankha Haucke, „dass die CISOs mit einem Anliegen in das Interview kommen. Fast alle scheinen etwas über sich und ihren Berufsstand sagen und erfahren zu wollen." Man wolle sich offenbar als CISO zeigen, erhoffe sich eine Würdigung des eigenen Tuns 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 schwierig erleben offenbar viele CISOs, dass man selbst nichts Konkretes produziert, was man vorzeigen und an dem man die eigene Wirksamkeit erleben und demonstrieren könnte. IT-Sicherheit ist zwar offenkundig notwendig, erzeugt aber keinen offenkundigen Mehrwert beziehungsweise steigert nicht offenkundig den Wert des Unternehmens. Eine frustrierte Aussage war: „Selbst die Putzfrau trägt dazu mehr bei, indem sie dafür sorgt, dass das Gebäude nicht ... schmutzig ist und die Kunden sich wohl fühlen."

Obwohl CISOs innerhalb ihrer Unternehmen zum größten Teil sehr engagiert in der Sache auftreten, befinden sie sich dennoch überwiegend in einem Dilemma: Sie müssen den ersten Analysen zufolge nach eigener Einschätzung eine „seltsame" Position ausfüllen und wirken zumeist im „Untergrund", wie aus einer „Zwischenwelt" heraus. In diesem Kontext beschreiben viele Teilnehmer der Studie ein ständiges Ringen mit sich – ein leidvolles

Erfahren, das nicht selten zu Identitätskrisen führt.

Schwieriger Perspektivwechsel

Und noch etwas wird deutlich: Die meisten Sicherheitsbeauftragte glaubten, ihr Unternehmen gut zu kennen, bevor sie – häufig auch ohne großes persönliches Zutun – in ihre jetzige Position gerieten. Dadurch wurden sie jedoch von jetzt auf gleich „ein anderer“: Die Perspektive des IT-Sicherheitsverantwortlichen änderte abrupt den Blick auf das vermeintlich Bekannte. Fast scheint es so, als hätten man als CISO etwas „Verzaubertes“ betreten, denn vieles wird plötzlich als „wie verhext“ beschrieben: Als CISO sollten die frisch Beförderten nun kontrollieren, bestimmen, Verantwortung tragen, sich ständig auf vielen verschiedenen Ebenen weiterbilden. Und sie sollen so tun, als gebe es nur Sicherheit – nichts anderes – und erst recht kein „Dazwischen“.

Dabei bleiben oftmals die Authentizität und somit auch Teile ihrer Kommunikationsfähigkeit beziehungsweise Glaubwürdigkeit bei denjenigen, die sie schützen sollen, auf der Strecke. Gerade diejenigen CISOs, die in ihrem Privatleben offensichtlich Risiken eingehen, scheitern der Studie zufolge am Vorleben einer Sicherheitskultur, die doch ihre Position ausfüllen sollte. Denn das „unsichere“ Leben, das manche in ihrer Freizeit führen, darf im Rahmen ihrer Arbeit als CISO keine Rolle mehr spielen – egal, ob man Wanderungen durch den Dschungel gemacht oder im familiären Umfeld das Risiko einer Großfamilie auf sich genommen hat.

Viele CISOs scheitern an der Compliance – auch an scheinbar entlastend gemeinten Vorgaben wie einer betrieblichen 80:20-Reglung (80 % Sicherheit, 20 % Risiko) –, weil am Ende trotz exakter Policy dennoch diffus erscheint, was mit den zu schützenden 80 % genau gemeint sein soll. So erscheint selbst ein vermeintliches Abrücken von dem 100%igen Ideal einer maximalen Absicherung eher als Be- denn als Entlastung.

Suche nach Imagekorrekturen

CISOs passiert immer wieder etwas Neues (Feuerwehrlogik). Hier zeigt sich eine Dynamik, bei der man permanent zwischen Sicherheit und Unsicherheit changiert, aber offensichtlich auch ein Zustand, in dem man sich durchaus einrichten und wohlfühlen kann. Allerdings verhindern das bloße Abdichten und die ständigen „Feuerwehr“-Einsätze ohne abschließende Auseinandersetzung mit den Geschehnissen das Ausbilden einer Sicherheitskultur mit klaren Vorgaben jenseits von Policy & Co. Somit arbeitet man unter anderem auch nicht an der Korrektur der „Bildlosigkeit“ des Berufsstands beziehungsweise an dessen „gutem“ Image. So äußerte ein CISO im Zuge seines Interviews schmunzelnd: „Zufriedenheit erreicht man selten, aber immerhin: Wenn man gute Arbeit macht, fällt man nicht auf.“ Der eine oder andere CISO wünscht sich, auch einmal ein explizites Lob zu bekommen.

Wie die originären Aufgaben des CISOs entspringen auch ihre Visionen offenbar keinem durchgängigen Bild: Bisweilen betrachtet er seine Arbeit im Kontext hoch aufgehängter Führungspositionen – dann wieder fühlt er sich beinahe wie ein „schräger Vogel“, quasi ganz unten. CISOs haben der Befragung zufolge nicht selten das Gefühl, nicht nur die Sache, sondern auch sich selbst schützen zu müssen. Nicht wenige kamen „gut gerüstet“ in die Interviews und legten ihre Verteidigung erst nach erheblicher Animation und fortgeschrittener Befragungszeit ab.

Aus diversen bildhaft beschriebenen „Leidenswegen“ haben sich schließlich verschiedene (vorherrschende) psychologische Umgangsformen, wie beispielsweise Selbstbeherrschung, Kameradschaft oder Undercover-Dasein, herausgebildet, die nach Abschluss der Analyse in der Anfang März erscheinenden

Endfassung der Studie für eine CISO-Typologie herangezogen werden sollen.

Froschkönige

Als vorläufiges Fazit kommentiert Projektleiter Udo Eichstädt: „Wir Morphologen nutzen gerne Märchen – im Bereich der Therapie wie auch im Change-Management für Unternehmen. Märchen werden von uns 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 dar – gerade auch der Arbeitswirklichkeit."

Im vorliegenden Fall der CISO-Studie scheint sich eine Analogie zum „Froschkönig" anzudeuten: „Der Umgang zwischen Prinzessin und Frosch bebildert ein Gefüge, das der Situation des CISOs zwischen dem in der Studie dargestellten ‚digitalen Prinzip' und dem ‚analogen Prinzip' ähnelt. Nach diesem Prinzip werden zwei zueinandergehörende Seiten als getrennt voneinander dargestellt – und dennoch drängt eine (unsichtbare) Kraft auf einen Austausch. Die in der Studie herausgearbeiteten Spaltungen in der Welt der Informationssicherheit lassen sich wechselseitig auf Prinzessin und Frosch verteilen", so Eichstädt weiter. Die Prinzessin steht dabei für das rein Digitale, das Unnahbare, den Eindruck des Besonderen, kultiviertes Verhalten, Kontrolle und „unbedarfte" Anwender – der Frosch symbolisiert banale Wirklichkeit, versteckt in seiner eigenen Welt, aber zugleich hilfsbereit, und außerdem Mitarbeiter, die nur die analoge Perspektive leben. ■

Dietmar Pokoyski ist Geschäftsführer der Kölner Kommunikationsagentur known_sense.

Der Berichtsband zur CISO-Studie ist ab Anfang März zum Preis von 380 € über den SecuMedia-Verlag (http://buchshop.secumedia.de) und known_sense erhältlich – <kes>-Abonnenten erhalten sie zum Sonderpreis von 290 €. Der offizielle Launch mit anschließender Podiumsdiskussion findet am 6. März von 10-13 Uhr im Heise-Forum auf der CeBIT statt (Halle 6/G 16). Ein Management-Summary der Studie erhalten <kes>-Leser im Mai als Beilage in der Ausgabe 2008#2.

Die Studie wird herausgegeben von der EnBW Energie Baden-Württemberg, known_sense, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro Deutschland; Idee und Feldarbeit stammen von known_sense – Medienpartner sind <kes> und securitymanager.de.