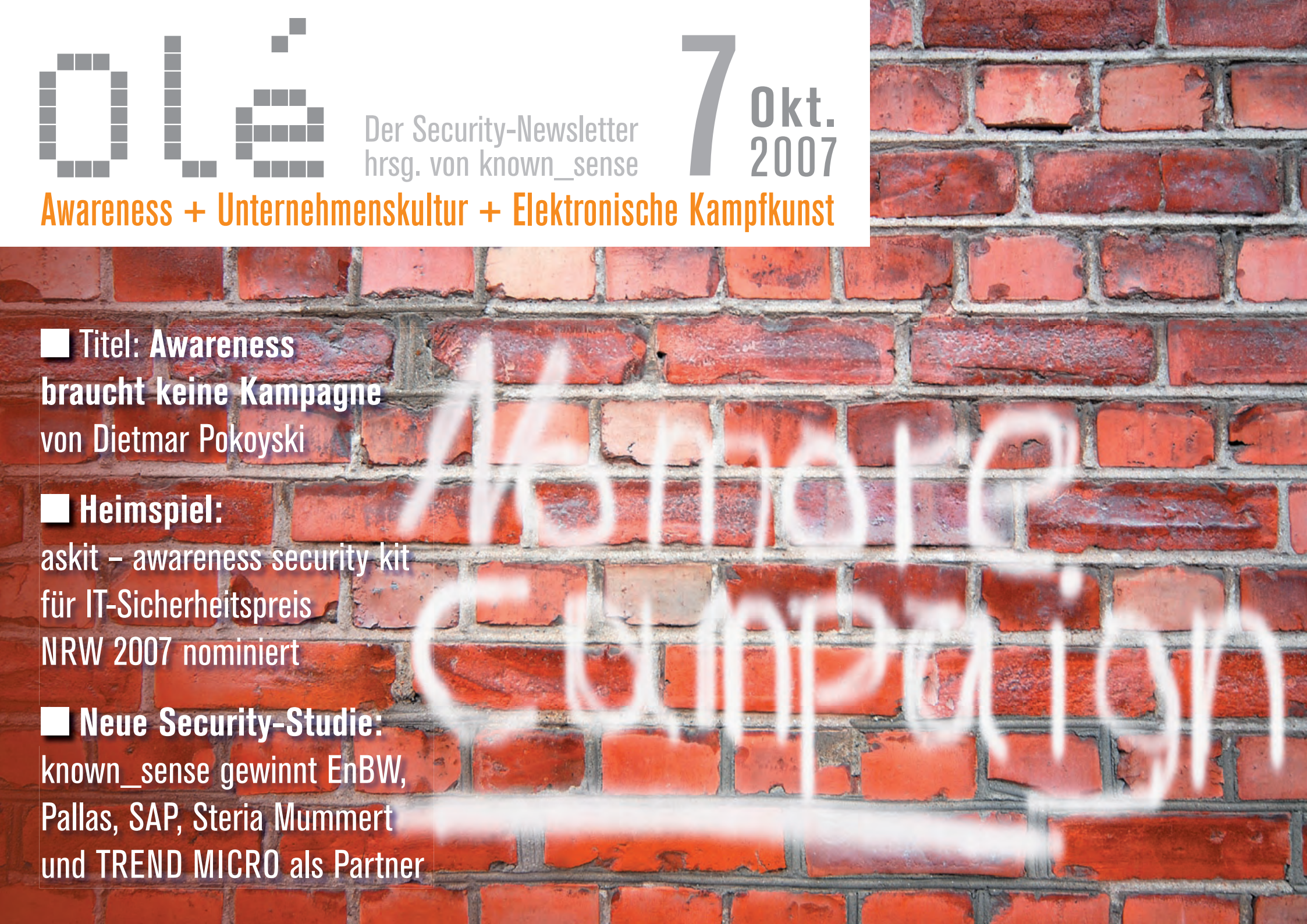
olé

Der Security-Newsletter
hrsg. von known_sense

7 Okt. 2007

Awareness + Unternehmenskultur + Elektronische Kampfkunst



- Titel: **Awareness braucht keine Kampagne**
  von Dietmar Pokoyski
- **Heimspiel:**
  askit – awareness security kit für IT-Sicherheitspreis NRW 2007 nominiert
- **Neue Security-Studie:**
  known_sense gewinnt EnBW, Pallas, SAP, Steria Mummert und TREND MICRO als Partner

Awareness braucht keine Kampagne!

Wer »Kampagne« sagt, muss auch »Entwicklung« meinen – manche Unternehmen fahren mit »Einzelmaßnahmen« besser

Ist von Security Awareness die Rede, geschieht dies überwiegend im Kontext des Begriffs Kampagne, der die Form meint, die Sensibilisierungsmaßnahmen zu einem logischen Ganzen verbindet. Stellt aber allein eine jede koordinierte Verdichtung einzelner Awareness-Maßnahmen gleich eine Kampagne dar bzw. was sind die Kriterien, die aus einer Serie von – vielleicht – Schulungs- und Trainingsveranstaltungen, von Medien oder von anderen Tools eine Kampagne werden lassen? Oder strategisch gefragt: Welchen Sinn macht eine derartige koordinierte Verdichtung? Kann nur eine Kampagne, bei der bereits im Vorfeld mit langer Hand jede Phase, jedes Detail geplant und ausgestaltet wird, nachhaltige Awareness schaffen? Oder können Einzelmaßnahmen, die zwar einer gewissen Dramaturgie gehorchen, nicht aber über eine kostenintensive Dachmarkenstrategie verbunden sind, nicht ebenso sinnstiftend wirken oder gar erfolgreicher sein?

Befragt man deutsche Unternehmen, die bereits Awareness-Kampagnen durchgeführt haben, nach Struktur und Dramaturgie ihrer Maßnahmen, stellt sich heraus, dass viele Kampagnen erschreckend gleichförmig aufgebaut sind und auf eine Architektur und Dramaturgie hinauslaufen, die schnell beschrieben ist: Unter einer Wortmarke mit (meist moralischem) Claim, die auf den Absender (IT-Abteilung, CSO, etc.) hinweist und in der mindestens einmal der Begriff »sicher«, ggfs. mit alternativem Wortstamm wie z.B. »sec…« vorkommt, werden über einen Gesamtzeitraum von 1,5 – 2,5 Jahren die 4, 5 oder 6 üblichen Verdächtigen der Security-Topics abgehandelt.

Das »Blockwart«-Prinzip

Dabei wird stets treudeutsch nach dem Hausmeister-Prinzip vorgegangen, d.h. zunächst wird ein Schild aufgestellt, dass man die neu gestaltete Rasenfläche ab sofort auch betreten darf (die so genannte »Kampagnen-Vorphase«, eine Art Minikampagne, die als Kick-off für die später folgende eigentliche Awareness-Kampagne wirbt, mithin Awareness für die Awareness). Sodann arbeitet man sich Etage für Etage und Wohnblock für Wohnblock vor, um etappenweise und en detail kundzutun, dass mit dem Betreten aber weder Fußballspielen, noch Radfahren, kein Grillen und erst recht kein Partymachen gemeint sei (die so genannten »Kampagnenblöcke«, die die o.g. gängigen Themen mehr oder weniger originell thematisieren und immer noch allzu oft mit einer Zeigefinger-Pädagogik daherkommen).

»Damit die Mitarbeiter nicht überrascht werden«

Auf Nachfrage, warum die Kampagne selbst vor dem Launch beworben werden muss statt für sich selbst zu sprechen, hört man dann als Argumente immer wieder O-Töne wie *»… damit klar ist, dass es sich hierbei NICHT um eine Leitbild-Kampagne handelt…«* oder *».. damit die Mitarbeiter nicht überrascht werden.«*

Huch! Nicht überrascht werden!? Da könnte dem »unmündigen Mitarbeiter« – ohne, dass dieser sich bewegt – doch glatt der Scheitel von links nach rechts rutschen.

Aber warum gerade hier der laute Ruf nach Vorsicht und offensichtlich so rigorosen Steuerungsprinzipien? So sehr Unternehmensführung und Change Management seit den 1990er Jahren bei Ihren Angestellten wie Kollegen mehr Eigenverantwortung fordern, so oft rutscht er dem einen oder anderen dann doch gerne wieder raus und desavouiert die oben genannte Forderung als einen banalen Versuch, Learnings aus dem letzten Management-Seminar oder →

der vorletzten Brand eins auch einmal im eignen Unternehmen abzusondern – Schöner Wohnen für Führungskräfte!

Das Goldene-Käfig-Prinzip

Hierzu passt auch der oftmals angeführte Vergleich, der Mitarbeiter mit Kindern gleichsetzt und für die Realisation bewusstseinsbildender Wirkung erzieherische Tricks anbietet. Erstens sind aber Mitarbeiter keine Kinder – zumindest dann, wenn das Unternehmen nicht Produktionsstätten in Indien und Umgebung betreibt. Und zweitens führt auch die Trickkisten-Pädagogik unvermeidlich zu einer Kultur, die einen Nährboden für Entsicherungsszenarien bietet, weil die Mitarbeiter den Trick in einem solchen Umfeld womöglich als Handlungsprinzip verstehen, aufgreifen und in der Regel bei Bedarf auch mal »gegen« das Unternehmen verkehren – wer sich ausgetrickst fühlt, sucht halt nach einem Ausgleich.

Dass eine solche Bevormundung auch keine absichernden Effekte erzeugt, sondern eher kontraproduktiv wirkt, kann man leicht aus dem Goldenen-Käfig-Prinzip – z.B. die Beziehung einer überbehütenden Mutter zu ihrem Kind – herleiten. Und auch die von known_sense initiierte tiefenpsychologische Securitystudie »Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen« propagiert einen Ansatz, der eine Bevormundung ablehnt: *»Die Mitarbeiter sollen sinnlich einbezogen werden durch eine lebendige, spannende Security mit Identifikationspotenzial«*, heißt es dort. Und: *»Awareness-Maßnahmen müssen eine Bilddramatik transportieren, wenn sie wirken wollen, und den Mitarbeiter darin als Mitstreiter erfahrbar machen.«*

Kultur der Angst

Unternehmer müssen aber nicht unbedingt die Psychologie bemühen, um einer solchen Argumentation folgen zu können. Allein der gesunde Menschenverstand sollte ausreichen, um zu sehen und zu verstehen, dass sich offenbar in zu vielen (deutschen) Unternehmen eine Kultur der Angst breit gemacht hat, die jede Form von Überraschung, jede spielerische Kommunikation und eben auch von Experimentellem verhindern will und Mitarbeiter eben nicht als Mitstreiter involviert sieht.

Dabei wird der unmündige Mitarbeiter oftmals mit dem unmündigen User gleichgesetzt bzw. daraus abgeleitet. Einen User-Tyus, den sich die Unternehmen durch den Einsatz unfertiger IT-Systeme und lückenhafter Prozesse selbst herangezüchtet haben. Der Umgang mit Fragmentarischem dürfte also denjenigen Mitarbeitern, die mit in der Regel halbgaren IT-Systemen hantieren, aus ihrem ganz normalen Arbeitsalltags durchaus bekannt vorkommen. Warum setzt also bei den meisten Unternehmern der Mut zur Lücke, zum Fragment, zum Experiment, den sie bei der Einführung der Systeme hegen, ausgerechnet bei den so wichtigen bewusstseinsbildenden Maßnahmen für die IT-Security aus?

Bei der Beantwortung dieser und anderer Fragen hilft womöglich auch ein kurzer etymologischer Exkurs. Das Wort Kampagne (französisch campagne: »Ebene« aus lateinisch campus: »flaches Feld«) wurde im 17. Jahrhundert in der Bedeutung von »Feldzug« in die deutsche Sprache übernommen. Diese Feldzüge waren in früheren Jahrhunderten zeitlich befristete Aktionen. Geht man außerdem davon aus, dass bei Feldzügen immer mindestens zwei Parteien aufeinander treffen, die sich bekämpfen, kann man viel von dem Selbstverständnis ableiten, mit dem heute in vielen Unternehmen Awareness-Kampagnen lanciert werden. CSO's stellen sich dabei nicht selten als Don Quichottes dar, die – vergeblich – gegen Windmühlen (Mitarbeiter) zu kämpfen scheinen. Und allein die Titel, Claims sowie die Ansprache dieser Kampagnen können in vielen Fällen nicht verbergen, dass da scheinbar immer noch »Krieg« geführt wird – nur sind Lanzen und Kanonen dem drohenden Zeigefinger, Kontrollen und Sanktionen gewichen.

In Awareness-Maßnahmen geht es aber weder um Krieg, und eben nicht nur um die Steigerung von Mitarbeiter-Bewusstsein in Bezug auf das Thema Security. Denn das Bewusstsein stellt – um mit der Terminologie eine Brücke zur Technik zu schlagen – nichts anderes dar als die so genannte front engine. Die so bedeutsame back engine von Awareness-Maßnahmen aber ist stets Entwicklung. Es geht also bei Awareness-Kampagnen – zumindest bei den guten – in erster Linie um Veränderungen. Um Entwicklung jedes einzelnen Mitarbeiters und um die Entwicklung des Unternehmens als Ganzes. Entwicklung, um zu einer unternehmensdienlichen Sicherheitskultur zu gelangen – um eine Entwicklung, die sich in einem fortwährendem Prozess befindet.

Veränderung betrifft alle

Dieser Entwicklung steht oft im Weg, dass in Unternehmen bisweilen eine latent groteske Vorstellung von Awareness herrscht. Analog zum Bild über den Kreativen, der gemütlich im Wald oder Park umherspaziert, bis die Idee ihn einfängt, glauben viele, das Bewusstsein für Sicherheit würde ihre Mitarbeiter nach dem Lesen von Flyern und Postern quasi wie an Pfingsten via herabregnender Feuerzungen erwischen. Und Veränderungen würden – wenn überhaupt – nur die Mitarbeiter betreffen und an den Absendern der Maßnahmen, den Securitymananagern und Geschäftsführern, vorbeigehen, weil diese ja qua ihrer Position bereits genügend über Risiken aufgeklärt wären.

Entwicklung wird aber nicht durch eine halbgare Post-PISA-Blockwart-Pädagogik angestoßen. Entwicklung ist – wie auch die Kreation guter Kommunikation – Arbeit und funktioniert nur im Kontakt mit anderen und mit sich selbst – inklusive der Sicherheitsbeauftragten und des Managements. Kontakte – vor allem dann, wenn es um Neues, um Überraschendes geht, um Positionierungsfragen und um ein offenes ➔

Miteinander, um Authentizität – stellen stets Grenzerfahrungen dar, die verständlicherweise beim einzelnen Angst erzeugen. Angst, die ausgehalten werden muss, will man mit dem Unternehmen wachsen und Sicherheitskultur kreieren.

Angst überwinden – Erregung kultivieren

Darüber hinaus ist die Vorstellung weit verbreitet, man könne Inhalte von Awareness-Kampagnen elegant an Themen vorbei lavieren, die problematische Unternehmensentwicklungen, z.B. Freisetzungen, Gehaltsverzicht, Kurzarbeit, etc., thematisieren.

Es gibt z.B. Consultants, die empfehlen Kunden, bei denen Entlassungen stattgefunden haben oder bevorstehen, doch allen ernstes, den Look einer Kampagne herunterzuschrauben, so dass die Mitarbeiter den eigentlichen Wert nicht mehr identifizieren können (ob Mitarbeiter wirklich so blöd sind, sei einmal dahin gestellt). Ich frage mich, was die CSO's, die einer solchen Logik folgen, eigentlich bezwecken. Wollen Sie trotz ihrer Kampagne einfach nur ihre Ruhe haben? Oder wollen Sie nicht eher eine derartige Situation der Unsicherheit und Unruhe, des Aufbruchs für Ihre Zwecke nutzen, um quasi HUCKEPACK Impact, Kommunikation, Involvement zum Thema Security mitzunehmen?

Aber vielleicht hat es sich noch nicht überall herumgesprochen: Die Menschen haben das Herumlügen und Herumtricksen satt. Der Angestellte von heute, der quasi ständig von der Entsicherung seines eigenen Arbeitsplatzes bedroht ist, will wissen, wo es lang geht. Da aber Awareness-Kampagnen nicht selten die einzigen Maßnahmen sind, mit deren Hilfe die Unternehmen heute mehr oder weniger professionell nach Innen kommunizieren, kommt ihnen eine besondere Bedeutung zu, d.h. Awareness-Kampagnen müssen mehr aufbieten als das Thema IT- oder Informationssicherheit. Sicherheitskultur sollte als Teil der Unternehmenskultur Zustände und Entwicklungen des jeweiligen Unternehmens auch über ihre originäre Themenvielfalt hinaus aus einer ganzheitlichen Sichtweise transportieren. Denn die durch Awareness-Maßnahmen oftmals beschworenen Topics wie Umsicht, Kontrolle oder Aufmerksamkeit betreffen selbstverständlich auch Bereiche, die sich jenseits einer auf Unternehmenssicherheit fixierten Kultur lokalisieren lassen – sprich: Was ist mit der Awareness für die soziale Sicherheit der Mitarbeiter? Was mit der, die dazu beiträgt, dass das Management nicht mehr so doofe Fehler macht und gar Jobs aufs Spiel setzt wie noch zuletzt? Und so weiter.

Grenzüberschreitungen als offener Prozess

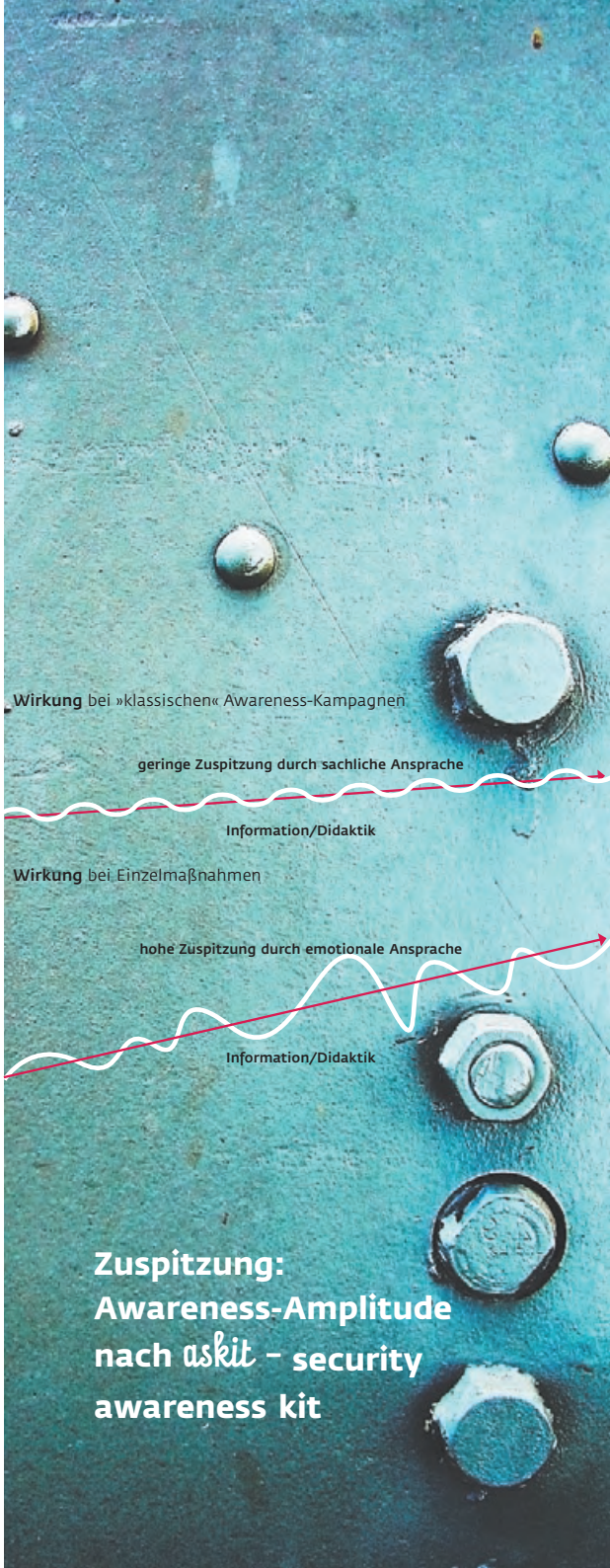
Leider überwiegt bei denjenigen, die über ihre Routinen hinaus nicht in der Lage sind, eine ganzheitliche Betrachtung Ihrer Unternehmungen, Grenzüberschreitungen zuzulassen, Überraschendes zu gestalten, die Angst. Und Unternehmen, in denen die Angst regiert, sind schlichtweg krank. Denn wenn man Erregung zu vermeiden versucht und eben nicht an seine Grenze geht, entsteht zuerst der Stau – und dann unwillkürlich Stillstand.

Dieser Effekt der Erregungsvermeidung gilt selbstverständlich für die gesamte Kommunikation innerhalb von Unternehmen – so auch für Awareness-Kampagnen, die, wenn sie keine wirklichen Überraschungen bieten, kontraproduktiv wirken, weil sie lediglich Stagnation füttern und somit langfristig Frustrationen bei den Mitarbeitern auslösen.

Nach einer Kampagne sollte eben vieles nicht mehr so sein wie vorher. Die eingeforderten Veränderungsprozesse betreffen aber auch diejenigen, die die Kampagne veranlassen und planen. Wer lediglich seine Kollegen und Mitarbeiter »erziehen« will, wer eine Awareness-Maßnahme MISSBRAUCHT, um Drohungen oder Sanktionen zu kommunizieren, wer Überraschendes zu vermeiden versucht, kann sich das Geld für eine Kampagne im Grunde sparen.

Fließende Übergänge

In dem Wissen um die Entstehungsprinzipien von Awareness und die eigene Sicherheitskultur und in dem Wissen um die Arbeit und die Prozesse, die mit einer Kampagne verbunden sind, erschließt sich der – zumindest zeitlich begrenzte – Vorteil von Einzel-Maßnahmen: Unter-➔



nehmen können, wenn ihre Maßnahmen nicht saisonal an statische Themenblöcke gebunden sind, kurzfristig auf Bedrohungen reagieren. Eine überbordene Erwartungshaltung bei Mitarbeitern, die z.B. nach der Ankündigung von Kampagnen stets vorhanden ist, wird gemindert, so dass auch Überraschungen planbar werden und das Gefühl der Penetration bei den Mitarbeitern nachlässt. Überraschungen führen zu höherer Erregung und zu Aufmerksamkeit. Und durch den Verzicht auf ein Kampagnen-CD (Corporate Design) können erhebliche Mittel eingespart werden, was aber nicht notwendigerweise weder gegen einen verbindenden Look bei Einzelmaßnahmen sprechen muss noch gegen eine strategische Ausrichtung dieser Maßnahmen – die Übergänge von Kampagnen zu Einzelmaßnahmen sind eben fließend.

Ob nun Einzel-Maßnahmen oder Kampagnen sinnvoll sind für Unternehmen, die Awareness erwarten, kann also nicht pauschal beantwortet werden. Die Antwort hängt von zahleichen Faktoren ab, u.a. von der Struktur, von Kooperationen des Unternehmens, von seinen Köpfen und der Unternehmenskultur, die diese prägen. Vom Wettbewerb, auf den man manchmal nicht so viel Einfluss hat, oder von der strategischen Weitsicht eines Unternehmens. Und rechnen Sie einmal nach: Gemessen an einem – vielleicht – halben Erwerbsleben eines Mitarbeiters stellen z.B. unterm Strich 4 oder 5 Awareness-Kampagnen in 25 Jahren letztlich auch nichts anderes dar als eine handvoll Einzelmassnahmen«.

Kampagne oder Einzelmaßnahmen? – Grundsätzlich gilt:

Kampagnen sind Einzelmaßnahmen grundsätzlich vorzuziehen, wenn ...

- ... sie stark dezentral agieren, die Mitarbeiter z.B. von zahlreichen Standorten aus wirken
- ... sie eine hohe Zahl an Individualisten beschäftigen
- ... sie Awareness als Enabler von Corporate Culture entdeckt haben und strategisch nutzen wollen
- ... sie von erheblichen Veränderungen betroffen sind, z.B. Fusionen, neue Kooperationen, Umstrukturierungen, einschneidenden personellen Veränderungen – auch Freisetzungen - , etc., und diese Veränderungen als Chance zugunsten einer optimierten Kommunikation nutzen wollen .

Die Voraussetzung für eine Kampagne inkludiert, dass man bereit ist, Entwicklungen resp. Veränderungen einzuleiten und ebenso wie für die Kampagne selbst frühzeitig eine Idee, eine Strategie für die Zeit danach existiert.

Unternehmen, die sich der benannten Defizite bewusst sind und diesbezüglich kurzfristig keinen adäquaten Ausgleich herstellen können, sollten auf Kampagnen verzichten und – wenn Sie dennoch Awareness erzeugen wollen – Einzelmaßnahmen planen.

Einzelmaßnahmen sind zu preferieren, wenn ...

- .. das Spielfeld für interne Kampagnen durch frühere (gescheiterte) Awareness-Kampagnen oder durch andere problematische interne Kommunikationsmaßnahmen, z.B. Leitbild-Kampagnen o.ä., verbrannt ist
- ... das Unternehmen aus verschiedenen Gründen nicht langfristig planen kann, z.B. bevorstehende, aber noch nicht spruchreife Veränderungen von Organisation (z.B. Fusionen), Struktur, Positionen, etwa eine nur vorübergehend besetzte Position des CSO's, etc.
- ... keine zufriedenstellende Zusammenarbeit mit strategisch wichtigen innerbetrieblichen Partnern zustande kommt, z.B. mit der Unternehmenskommunikation oder der Mitarbeitervertretung, etc.
- ... eine rigorose CI keine Line-Extender des Corporate Designs für den internen Gebrauch einzelner Unternehmensteile zulässt
- ... der Kontext zwischen Sicherheitskultur und Unternehmenskultur nicht erkannt bzw. geleugnet wird und entscheidende Veränderungsprozesse im Grunde unerwünscht sind

Ausnahme: Unternehmen, die das Thema Security Awareness äußerst selbstbewusst und mit erheblicher strategischer Weitsicht, z.B. länger als über einen durchschnittlichen Kampagnen-Zeitraum von ca. 1,5-2,5 Jahren, behandeln, erkennen das Potenzial eines offenen Prozesses und produzieren quasi eine Never-ending-Awareness-Tour als Meta-Kampagne mit strategisch aufeinander abgestimmten »Einzelmaßnahmen«.

Mit dem Management-Tool askit – awareness security kit, das für den IT-Sicherheitspreis NRW 2007 nominiert ist (s. n. S.), hat known_sense ein Analysetool kreiert, mit dem jedes Unternehmen in der Lage ist, Sicherheitskultur zu identifizieren und die Maßnahmen zielgenau zu planen. Mithilfe von askit kann auch eruiert werden, welche Art von Maßnahmen für das jeweilige Unternehmen sinnvoll ist. Kampagne oder Einzelmaßnahmen – am Ende zählt vor allem eines: die Überraschung, das Emotionale, das Involvement. Effekte, die den Erfolg und die nachhaltige Wirkung bestimmen – unabhängig davon, ob sie durch Kampagnen erzielt wurden oder nicht. Effekte, die die sich aber in der Regel nicht ein oder zwei Jahre im voraus planen lassen – und in einem schnelllebigen Feld wie der IT-Security schon gar nicht. ■

known_sense für IT-Sicherheitspreis NRW 2007 nominiert

Heimspiel: Tool »askit – awareness security kit« wird am 21.11.2007 in Köln ausgezeichnet

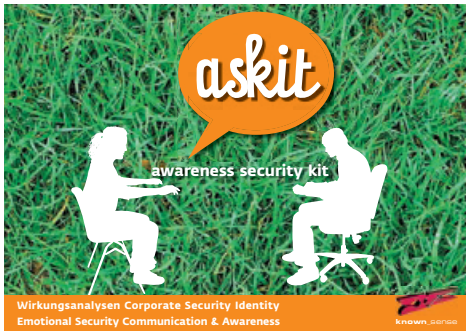
Die Kölner Kommunikations- und Consulting-Agentur known_sense wurde von der Jury der Landesinitiative »secure-it.nrw« wie bereits vor zwei Jahren für den »IT-Sicherheitspreis Nordrhein-Westfalen« nominiert und wird am 21. November 2007 im Rahmen des »6. IT-Sicherheitstages NRW« in Köln vom Innovationsminister Prof. Dr. Andreas Pinkwart für einen vorbildlichen Beitrag zur Informationssicherheit ausgezeichnet.

Galt die Auszeichnung 2005 noch für die Kategorie »Bildung« und für ein Gemeinschaftsprojekt mit den angehenden Designern der Fachoberschule für Gestaltung in Köln, die im Rahmen einer Projektkooperation von Schule und Agentur Konzepte und Dummies für Security-Awareness-Tools produzierten, erfolgt die Nominierung in diesem Jahr in der Kategorie »Mittelstand«.

»Das Thema IT-Sicherheit wird von vielen als unbelebt grau oder theoretisch abgehoben wahrgenommen und hat daher ein überwiegend negatives Image«, bedauert Dietmar Pokoyski, Gründer und Geschäftsführer von known_sense, »das erschwert die Implementierung und die Steuerung einer nachhaltige Wirkung von Schutzmaßnahmen in Unternehmen«. Für Pokoyski folgert daraus aber nicht, dass Mitarbeiter noch häufiger geschult oder etwa überwacht werden müssen. Er plädiert für offene Clients bzw. mehr persönlichen Freiraum an jedem PC-Arbeitsplatz. Sein Plädoyer stützt sich auf die Erkenntnisse einer Grundlagenstudie zum Thema Informationssicherheit in Unternehmen aus dem Jahr 2006.

Im letzten Jahr hatte ein von known_sense beauftragtes Psychologen-Team im Rahmen der Studie »Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen« die Psychologie der Informationssicherheit entschlüsselt.

Aus welchen Gründen machen Mitarbeiter Fehler, die IT-Systeme in Unternehmen entsichern, wollten die Forscher wissen und fanden Überraschendes heraus: Es ist selten Unwissenheit, die kognitiv, z.B. über Schulungen, zu beheben wäre. »Die meisten Mitarbeiter wissen sehr wohl, was richtig und falsch ist«, erläutert Dietmar Pokoyski. »Fehler passieren«, haben die psychologischen Projektleiter der Studie, Ankha Haucke und Udo Eichstädt, herausgefunden, »u.a. als unbewusste Befreiungsschläge, wenn z.B. technische oder organisatorische Maßnahmen als zu einengend wahrgenommen werden.« Die Paradoxie: Je dichter das Sicherheitsnetz eines Unternehmens ist, umso mehr versuchen die Mitarbeiter dieses System – unbewusst – zu durchbrechen, um sich des menschlichen Faktors, der in zahlreichen Unternehmenskulturen nur noch marginal vorhanden ist, zu vergewissern und damit Ihre eigene Arbeitsleistung zu erhalten.



Auf Grundlage dieser und der aktuellen Studie (s.n.S.) können Unternehmen und Dienstleister der IT-Branche Learnings generieren, die dazu beitragen, Sicherheitskultur entscheidend zu optimieren. Auf der Grundlage dieser Forschung haben Pokoyski und Mitarbeiter aber auch das für den IT-Sicherheitspreis NRW nominierte Management-Tool entwickelt, das Sicherheitskultur in Unternehmen analysieren und proaktiv gestalten lässt. Das »Baukastensystem« mit dem Namen »askit – awareness security kit« schlägt ein psychologisch fundiertes Verfahren vor, mit denen ein Unternehmen ein CSI→

IT-Sicherheitspreis NRW

Informationssicherheit und Datenschutz sind sensible Bereiche der Informationstechnik. Hier setzt der »IT-Sicherheitspreis NRW« an, der von der Landesinitiative »secure-it.nrw« und dem Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen vergeben wird. Ausgezeichnet werden kleine und mittelständische Unternehmen – Anwender und Anbieter – mit beispielhaften und innovativen Lösungen. Hierbei kann es etwa um die Entwicklung einer Technik gehen, um Sensibilisierungsmaßnahmen oder die Optimierung von Abläufen. In der Kategorie »Mittelstand« sind in diesem Jahr drei, in der Kategorie »Bildung« zwei Beiträge nominiert, von denen jeweils einer den IT-Sicherheitspreis erhält. Die nominierten IT- und Datenschutzlösungen werden über eine umfangreiche Broschüre und weitere Kommunikationsmaßnahmen einer breiten Öffentlichkeit vorgestellt.

(Corporate Security Identity) identifizieren und optimieren kann. Analyse, Beratung, Coaching und Kreation sind die Hauptbestandteile von »askit«. In der Analyse, die z.B. auch zweistündige Tiefeninterviews und Gruppendiskussionen beinhaltet, können verdeckte Motive aufgespürt werden, die das Verhalten der Mitarbeiter im Umgang mit u.a. IT und sensiblen Daten beeinflussen. Ein Gutachten dokumentiert die Ergebnisse der Analyse und liefert die Basis für den nächsten Schritt, der Consulting bzw. das speziell für Sicherheitsbeauftragte entwickelte Coaching »rosi« umfasst. Innerhalb des Beratungsprozesses werden dann gemeinsam strukturelle Verbesserungen von Sicherheitskultur im Unternehmen entwickelt und schließlich im dritten Schritt, der Kreation von innovativen Awareness-Maßnahmen bis hin zu Kampagnen, umgesetzt.

Storytelling & Game Based Development

Neben der tiefenpsychologische Methode setzt known-sense vor allem narrative Managementkonzepte (z.B. Storytelling bzw. Story Management) und Game Based Development ein, eine Methode die Spieldynamiken nutzt, um im Rahmen von z.B. Change Management nachhaltige Veränderungsprozesse in Unternehmen einzuleiten. Auch hierfür hat die Agentur zwei Tools entwickelt, auf der wiederum Teile von »askit« aufbauen, »chambs – change management braucht story« und »trumps – tools & rules für unternehmensmanagement- & -prozess-spiele«.

Damit behandelt mit »askit« erstmals ein Tool Unternehmenssicherheit und die hiermit verbundenen Risiken im Kontext aller relevanten Faktoren – »auch derer, die auf den ersten Blick nicht unmittelbar zum Security-Arbeitsumfeld zu gehören scheinen«, sagt Dietmar Pokoyski. Der Diplom Psychologe Udo Eichstädt ergänzt: »Jedes Unternehmen produziert seine individuelle Sicherheitskultur, die untrennbar mit der Kultur des Unternehmens verbunden ist. Dies hat Konsequenzen für die Ausrichtung jeglicher Kommunikation, die Sicherheit zum Thema hat. Entsicherndes Verhalten lässt sich nicht als isoliertes Phänomen verstehen, dass es mit allen Mitteln zu beseitigen und verhindern gilt. Vielmehr ist die Frage zu stellen, welcher Sinn in einem bestimmten Verhalten zum Ausdruck kommt. Technisch geprägte Lösungen behandeln stets nur die Symptome der Sicherheitslecks, nicht aber die wirklichen Ursachen.« ■

Neue CSO-Studie

EnBW, SAP, Steria Mummert, Pallas und Trend Micro Partner

Am 9. November startet die Feldarbeit zur CSO-Securitystudie, die known_sense gemeinsam mit der EnBW, Pallas, SAP, Steria Mummert Consulting und Trend Micro sowie den Medienpartnern <kes> – Die Zeitschrift für Informationssicherheit und securitymananger.de produziert.

Hierbei handelt sich um eine tiefenpsychologische Analyse von Securitymanagern mit dem Arbeitstitel: »Aus der Abwehr in den Beichtstuhl – der Sicherheitsbeauftragte zwischen Seelsorger und Doppelagent. Image- und Positionierungsanalyse CSO & Co.«.

Ein dreiköpfiges Team, bestehend aus erfahrenen Diplom-Psychologen und Marktforschern wird insgesamt 30 zweistündige face-to-face-Tiefeninterviews im Köln-Düsseldorf-Bonn-Aachen durchführen.

Die Studie erscheint rechtzeitig zur cebit Anfang März 2008 und ist zum Preis von Euro 380,00 (Subskr.preis bis 15.03.2008 Euro 290,00) über die <kes> oder known_sense zu beziehen. Unmittelbar im Anschluss an den Launch sowie im Rahmen der SYSTEMS 2008 sind zwei Roundtables mit den Herausgebern sowie ausgewählten CSO's geplant. ■

Olé Nr. 8 erscheint im Anfang 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