„Entsicherung am Arbeitsplatz – Studie entschlüsselt erstmalig psychologische Wirkweise und Zusammenhänge der IT-Security"

Tiefenpsychologische Pilotstudie „Entsicherung am Arbeitsplatz" belegt: Einhundertprozentige Sicherheit ist von Menschen nicht auszuhalten.

München, 23. Oktober 2006. **„Der Wunsch eines jeden IT-Security Officers ist ein absolut sicheres Unternehmen – und ein Computernetzwerk, das dicht hält. Doch so, wie sich in einem Neubau mit modernster Architektur schnell Schimmel bildet, lüftet man ihn nicht regelmäßig kräftig durch, so entstehen in einem solch vermeintlich sicheren IT-System schon nach kurzer Zeit seelische Wucherungen", fasst Dietmar Pokoyski die erste tiefenpsychologische Security-Studie „Entsicherung am Arbeitsplatz – Die geheime Logik der IT-Security in Unternehmen" heute während einer Pressekonferenz auf der SYSTEMS in München zusammen. Der Geschäftsführer der Kölner Kommunikationsagentur known_sense und Initiator der Pilotstudie ging gemeinsam mit den weiteren Herausgebern, der EnBW Energie Baden-Württemberg AG, der Deutschen Sparkassen Verlag GmbH, <kes> – Die Zeitschrift für Informationssicherheit, der Pallas GmbH und nextsolutions auf Spurensuche nach den psychologischen Wirkungen innerhalb der IT-Security.**

„Wir erleben immer wieder, dass den Kunden zwar bewusst ist, dass IT-Sicherheit nötig ist, die Umsetzung von Sicherheitsmaßnahmen schließlich aber doch zu kurz kommt oder nicht greift", sagt Dr. Kurt Brand, Geschäftsführer des Brühler IT-Dienstleisters Pallas GmbH. „Als Partner dieser Untersuchung lag uns am Herzen, mehr über die psychologischen Faktoren zu erfahren, die das Sicherheitsbewusstsein tatsächlich prägen."

Seit die Informationstechnologie Einzug in die Unternehmen gehalten und die Entwicklung von Security-Routinen ihre Handhabung zum Tagesgeschäft erkoren hat, gelten Irrtum und Nachlässigkeit der eigenen Mitarbeiter als die primären Gefahrenquellen im System. Die Ursachen dieser „Fehlleistungen" – so das gängige Schlagwort – blieben bis dato jedoch unerforscht.

Robert Kaltenböck, Abteilungsleiter IT-Consulting in der Geschäftssparte Systemhaus des Deutschen Sparkassenverlags, der die Unternehmen und Verbände der Sparkassen-Finanzgruppe umfassend im Bereich IT-Sicherheitsmanagement, Web Based Training IT-Sicherheit, Business Continuity Management/Notfallvorsorge und Mobile Security unterstützt, sagt: „Besonders für Sparkassen, die mit sehr sensiblen Daten arbeiten, sind Zuverlässigkeit und Sicherheit des IT-Betriebes das A und O und damit wesentliche Erfolgsfaktoren. Erkenntnisse, die uns helfen, aktuelle Kundenbedürfnisse und neue Marktanforderungen in unsere Lösungen einzuarbeiten, sind für uns von großer Bedeutung."

Was also sind die ‚geheimen' Faktoren, die vermeintlich sicheren IT-Systeme immer wieder auszuhebeln drohen? Auf Basis morphologischer Markt- und Medienforschung befragte im Sommer 2006 ein anerkanntes Psychologen-Team in jeweils zweistündigen Tiefeninterviews Angestellte nach ihren Gewohnheiten und Wünschen im Umgang mit ihrer IT-gestützten Arbeit und nach ihren Vorstellungen von IT-Security und Unternehmenskultur.

Mit beeindruckendem Ergebnis: Unternehmen, die immer weniger rein und auch immer weniger raus lassen, minimieren ihre Entwicklungschancen und die Ihrer Mitarbeiter. Durch technologische Innovationen zunehmend sachlich geprägte Arbeit, die immer weniger Eigenes, immer weniger Menschliches zulässt, erscheint leblos und fade.

Entsicherung am Arbeitsplatz

IT-Security als Enabler der Unternehmenskultur

Und noch etwas wird in der Studie deutlich: IT-Security beeinflusst die Unternehmenskultur in entscheidendem Maß. Wird ihre Schutzfunktion auch als positiv und notwendig erachtet, so verkehrt sich dieser Schutz nicht selten in ein Zwangsystem, das Identität und individuelle Gestaltungswünsche der Mitarbeiter ausschließt: „Auf der Arbeit habe ich nichts Persönliches auf dem PC, weil ich davon ausgehe, dass die EDV mich durchleuchten kann", sagt ein Teilnehmer der Studie.

Der Umgang mit IT-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 – „Ich mache schon mal Sachen auf, z.B. 13 Sprüche für die Seele – mit Bildern. Einfach, damit es einem gut geht" – wird zum unbewussten Befreiungsschlag gegen die Unternehmenskultur im allgemeinen und die IT-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.

Seele greift in die Trickkiste

Pokoyski findet für diese psychologische Dimension ein bekanntes Bild: „Die Seele greift tief in ihre eigene Trickkiste und umdribbelt mit brasilianischer Leichtigkeit alles Rationale." Dabei verkehrt sich das im Rahmen der Untersuchung entdeckte Phänomen des Sachlichen Verschliessens (Schutz vor Ein- und Ausbrechern) in Ausbrüche, die dem Prinzip des Menschlichen Eröffnens folgen: Bei Mitarbeitern, die die zunehmende Entmenschlichung von Arbeit nicht länger aushalten, kommt es unbewusst zu bekannten Fehlleistungen, bei dem sich die Mitarbeiter nicht nur sich selbst, sondern auch ihr Unternehmen regelrecht entsichern.

Und doch: Die Entsicherung am Arbeitsplatz stellt im Grunde etwas ‚Gutes' dar, dient sie doch der Versicherung der eigenen Identität. Die Mitarbeiter begehen mithin ‚Fehler', um durch das hiermit verbundene Menschliche Eröffnen ein wenig Menschliches in ihre Arbeit zu retten und damit ihre persönliche Produktivität zu sichern. Mitarbeiter und Unternehmen können an dieser Stelle in dem Wissen um die eigentlichen Ursachen aber auch Verbündete im Dienst der eigenen Sache werden und so Zuverlässigkeit und Sicherheit des IT-Betriebes nachhaltig stärken.

Um dieses Ziel zu erreichen, empfiehlt die Studie Unternehmen, sich zu immunisieren, indem sie das Menschliche Eröffnen, die emotionalen und zum Teil schrägen Seiten der Mitarbeiter akzeptieren und sogar fördern. Die Unternehmenskultur muss Ausbrüche zulassen und versuchen, diese so gut wie möglich zu steuern. Gute und lebendige Awareness-Kampagnen, die eher im Unbewussten wirken, werden in diesem Zusammenhang wichtiger als offene Drohungen oder endlos wirkende IT-Schulungen. Entscheidend ist also der Impfstoff, den sich das Unternehmen mixt. Mit ausgewogenen Mitteln wird es das eigene Immunsystem stärken und damit im wahrsten Sinne des Wortes virenfrei bleiben – ohne die Substanz, die Mitarbeiter, nachhaltig zu schwächen. „Frei nach dem Motto ‚Einzeln sind wir Worte – zusammen ein Gedicht', ergänzt Wolfgang Reibenspies, IuK Security Manager und Konzernbevollmächtigter IuK-Security bei der EnBW.

Menschlicher Faktor gesetzt

„IT-Security muss sich mit Menschlichem aufladen und Identifikationsinhalte schaffen, um allzu sachlich geratene Awareness-Kampagnen zu optimieren. IT-Security braucht eine Story. Braucht Protagonisten. Muss für sich werben. Die Mitarbeiter sind bereit zu kämpfen. Man muss sie aber auch lassen", diktiert Dietmar Pokoyski den Sicherheitsentscheidern ins Hausaufgabenheft. Denn dann, so Pokoyski, „klappt es auch mit der ‚Defense'. Dann wird IT-Security nicht nur Teil der Unternehmenskultur sein, sondern diese sogar entscheidend prägen."

Die ersten Unternehmensverantwortlichen reagieren begeistert auf die Erkenntnisse der Studie. Wolfgang Reibenspies (EnBW) sieht sich durch sie in seiner Auffassung, dass IT-Security ein Teil der Unternehmenskultur sein muss, bestätigt und ergänzt, „dass wir in der IT-Security nur dann etwas verändern werden, wenn wir die Menschen erreichen und abholen. Auch, wenn der Security-Manager nie der beliebteste Mann im Unternehmen sein kann, so kann er doch folgendes vermitteln: Nur wenn der Wert der Informationen, Daten und Systemkomponenten für den Fortbestand des Unternehmens und seiner Marktposition auf allen Ebenen – im Management und gleichermaßen wie bei den Anwendenden – verstanden wird, werden die Mitarbeiterinnen und Mitarbeiter diese auch schätzen und damit schützen können. Die Studie kommt genau zum richtigen Zeitpunkt. Ihre Erkenntnisse sollen in die Arbeit der EnBW einfließen, da ich diese für außerordentlich wichtig erachte." Seiner Meinung nach bietet die Studie „viel, viel Stoff zum Nachdenken".

Die Studie, deren Forschungsansatz 2007 auf weitere Security-Felder ausgedehnt wird, kann zu einem Preis von € 380,00 (Subskriptionspreis bei Bestellungen bis zum 31.10.2006 € 290,00) über <kes> oder known_sense bestellt werden. Eine englische Version ist ebenfalls verfügbar.

Kasten 1: DSV-Gruppe
Die DSV-Gruppe, die sich aus dem Deutschen Sparkassenverlag sowie seinen Tochter- und Beteiligungsunternehmen zusammensetzt, zählt mit einem Jahresumsatz von rund 713 Millionen Euro (2005) zu den zehn umsatzstärksten Medienhäusern Deutschlands. Als spezialisierter Lösungsanbieter für die Verbände und Unternehmen der Sparkassen-Finanzgruppe bietet die DSV-Gruppe klassische Verlagsmedien wie Bücher, Ratgeberreihen, Fach- und Kundenzeitschriften sowie organisatorische Medien wie Vordrucke, technische Geräte und Bankkarten. Ergänzt wird das Leistungsportfolio durch informatikgestützte Dienstleistungen, Internet-Angebote, elektronische Beratungssysteme sowie Full-Service-Agenturleistungen inklusive Kommunikationskonzepte und PR-Events. Das Unternehmen beschäftigt 1.660 Mitarbeiterinnen und Mitarbeiter. Hauptsitz der DSV-Gruppe ist Stuttgart-Vaihingen, darüber hinaus ist das Unternehmen bundesweit an zahlreichen Standorten vertreten. http://www.dsv-gruppe.de

Kasten 2: EnBW Energie Baden-Württemberg
Die EnBW Energie Baden-Württemberg AG mit Hauptsitz in Karlsruhe ist mit rund fünf Millionen Kunden das drittgrößte deutsche Energieunternehmen. Mit derzeit rund 17.800 Mitarbeiterinnen und Mitarbeitern hat die EnBW 2005 einen Jahresumsatz von 10.769,3 Millionen Euro erzielt. Die Kernaktivitäten konzentrieren sich auf die Geschäftsfelder Strom, Gas sowie Energie- und Umweltdienstleistungen. Die EnBW ist föderal organisiert, die Organhaftung liegt bei den Gesellschaften. http://www.enbw.com

Kasten 3: <kes> – Die Zeitschrift für Informations-Sicherheit
Die 1985 gegründete <kes> enthält unter anderem das offizielle Organ des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Sie ist eine der bedeutendsten deutschsprachigen

DSV Gruppe Deutscher Sparkassenverlag · EnBW · <kes> Die Zeitschrift für Informations-Sicherheit · known_sense · nextsolutions · pallas

Fachzeitschriften zum Thema IT-Security. <kes> erscheint sechs Mal im Jahr im SecuMedia Verlag (wie auch die WIK – Zeitschrift für die Sicherheit der Wirtschaft), der u.a. auch Veranstalter der IT-SecurityArea auf der SYSTEMS ist. http://www.kes.info

Kasten 4: known_sense

Die Kölner Agentur known_sense ist Full-Service-Dienstleister für Kommunikationsprojekte aller Art – u.a. auch im Grenzbereich zwischen den Topics „Sicherheit" und „Spielen". So kreiert known_sense etwa zeitgleich Awarenesskampagnen für Unternehmen aus dem Finanz- bzw. Energiebereich oder Neuprodukte für Spieleverlage wie ASS Altenburg, für Mattel oder Disney. Qualitative Marktforschung, Beratung und Coaching – vor allem für die IT-Branche – runden das Portfolio ab. 2004 produzierte man den bekannten Security-Awareness-Klassiker „Das Virusquartett". 2005 wurde die Agentur für einen vorbildlichen Beitrag zur Informationssicherheit beim NRW-Sicherheitspreis ausgezeichnet. Im November ist known_sense Mitveranstalter des Expertenforums und Security-Stammtisches „WÖLFE & GEISSEN" in Köln. Z.Z. entwickelt man u.a. auch das Tool „Awareness Security Kitt" (ASK) und das Mitarbeiter-Awareness-Magazin „Olé". http://www.known-sense.de http://www.virusquartett.de

Kasten 5: nextsolutions

Die Marketing- und Technologieberatung nextsolutions ist auf das Thema Security Awareness spezialisiert. Die Kernkompetenz liegt darin, innerhalb von Unternehmen eine aktive Sicherheitskultur zu etablieren. Inhaber Marcus Beyer ist zudem Chefredakteur der Online-Fachmagazine Securitymanager.de, VoIPmagazin.de und KlinikITmanager.de. http://www.nextsolutions.de

Kasten 6: Pallas

Die Brühler Pallas GmbH sorgt für professionelle und umfassende Internet-Sicherheit zu festen Mietpreisen und entwickelt sichere Lösungen für den internetbasierten Wissensaustausch, für E-Learning sowie für die Kommunikation und Interaktion im Web. Das Produkt Managed Security Service gewann 2003 den ASP Award und bietet Firewall-Schutz gegen Hacker und Viren, gegen Spam und unerwünschten Inhalt, dazu Intrusion Detection und starke Authentifizierung. 2004 wurde Pallas für einen vorbildlichen Beitrag zur Informationssicherheit beim NRW-Sicherheitspreis ausgezeichnet. http://www.pallas.com

7.500 Zeichen (ohne Infokästen)

Diese Information als PDF:

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

Weitere Informationen, die Management-Summary der Studie und Bildmaterial auf Anfrage oder zum downloaden hier:

Studien-Auszug (10 S., PDF, 50 dpi, 2,8 MB):

http://www.known-sense.de/entsicherung/securitystudie_auszug_50dpi.pdf.

Factsheet (1 S., PDF, 72 dpi, 1,1 MB):

http://www.known-sense.de/entsicherung/securitystudie_factsheet_72dpi.pdf

Abbildung Cover Berichtsband (JPG, 300 dpi, 0,2 MB)

http://www.known-sense.de/entsicherung/securitystudie_cover.jpg

Abbildung Infografik „Psychologie der IT-Security" (JPG, 300 dpi, 0,4 MB)

http://www.known-sense.de/entsicherung/entsicherung_infografik.jpg

Kontakt: known_sense Dietmar Pokoyski
Kaiser-Wilhelm-Ring 30-32 D-50672 Köln Fon +49 221 91277778 sense@known-sense.de

Entsicherung und Abrechnung

DSV Gruppe Deutscher Sparkassenverlag · EnBW · <kes> Die Zeitschrift für Informations-Sicherheit · known_sense · nextsolutions · pallas