known_sense

VIRUSQUARTETTDE

TOOLS & SERVICES
FÜR SECURITY-MANAGEMENT & -PROMOTION

SECURITY-NEWSLETTER 04 OKT.2006

Studie entschlüsselt erstmalig psychologische Wirkweise und Zusammenhänge der IT-Security

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. Pilotstudie „Entsicherung am Arbeitsplatz - Die geheime Logik der IT-Security in Unternehmen" produziert.**

„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 Marktanforde-

Die Themen

Impressum

Herausgeber:
Dietmar Pokoyski (known_sense)
Kaiser-Wilhelm-Ring 30-32
D-50674 Köln
Fon +49 221 91277778
securitytools@known-sense.de
www.virusquartett.de
www.known-sense.de
Fotos S. 2-4 (l.): www.Photocase.com

rungen 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.

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 blei-

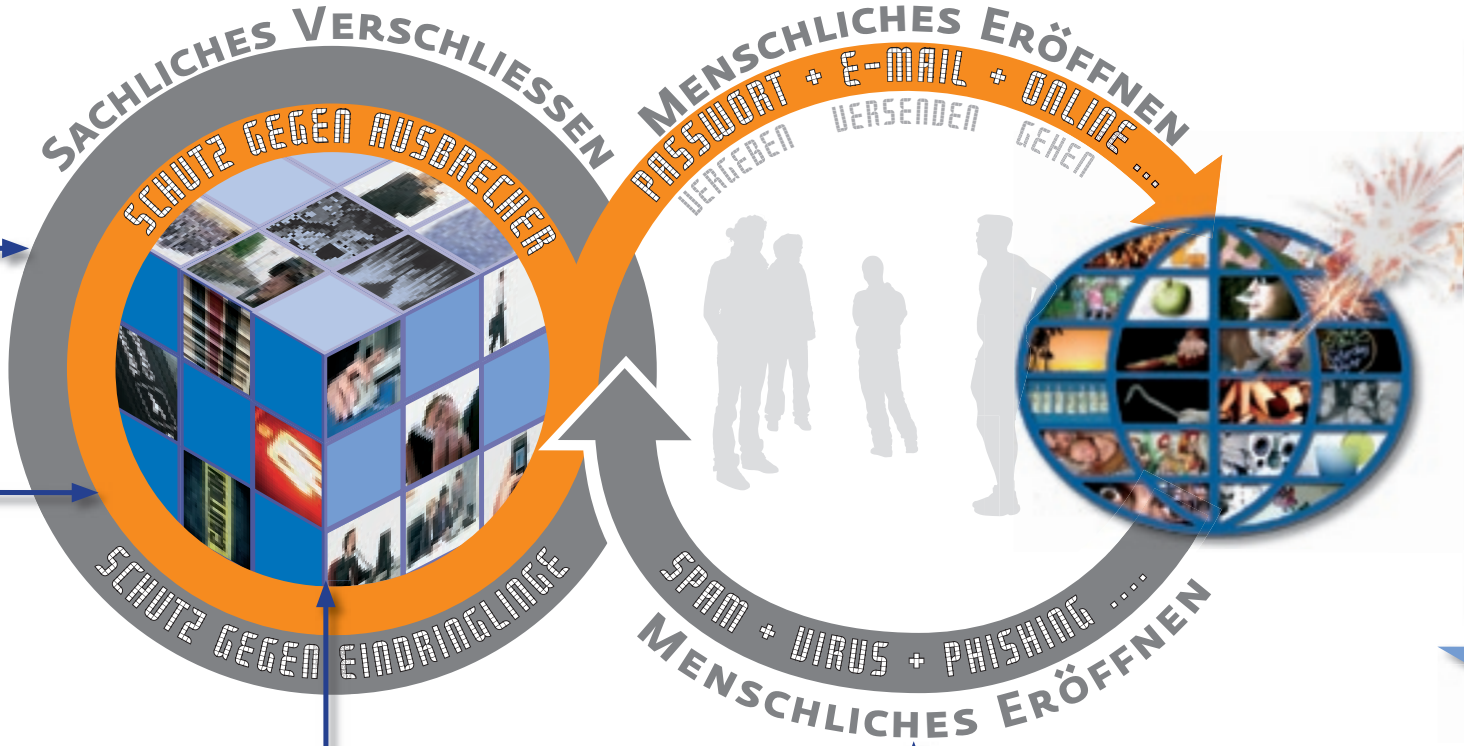
ENTSICHERUNG AM ARBEITSPLATZ

Psychologie der IT-Security

Sicherung und Erhalt einer funktionierenden Einheit **(Schutz gegen Eindringlinge)**

&

Sicherung und Erhalt einer sachdienlichen Verfassung **(Schutz gegen Ausbrecher)**



Unternehmens-kultur bietet zu wenig Raum für ein selbstverständ-liches Unterbringen von Eigenem.

–

IT-Security spitzt die Ver-Sachlichung in ihren derzeitigen Maßnahmen zu.

Not-Lösung

Verkehrungs-gefahr

Ver-Sachlichung (menschlicher Identität)

Fehlleistungen

Verschiebungen

Ent-sicherung am Arbeitsplatz

ben – 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.

Ihre Studien-Bestellung richten Sie bitte an sense@known-sense.de. ■

Dietmar Pokoyski (known_sense): „Die Seele greift tief in ihre eigene Trickkiste und umdribbelt mit brasilianischer Leichtigkeit alles Rationale."

Wölfe & Geissen

Der Rheinische Security-Stammtisch

Außerhalb und unabhängig von Institutionen wie IHK's und Online-Communities wie etwa Open BC soll jetzt der Rheinische Security-Stammtisch DAS Forum sein, das Experten aus unterschiedlichen Richtungen die Möglichkeit eröffnet, die Topics „Security" und „Unternehmenskultur" ohne disziplinäre Begrenzung zu diskutieren.

Der Titel „WÖLFE & GEISSEN" ist dabei durchaus programmatisch zu verstehen. Wie alles im Leben - auch das zeigt die o.g. Sicherheitsstudie - hat auch die Security, haben auch ihre Protagonisten immer zwei Seiten: sie sichern und entsichern zugleich! Und in dem Grimm'schen Märchen, auf das der Titel Bezug nimmt, finden sich Sicherung und Entsicherung sowie Hinweise auf alle weiteren Aspekte, die das Security-Terrain abstecken: Kontrolle, Täuschen, Infizieren, Phishen, Verstecken, Entlarven, etc.

Aber auch das RHEINISCHE ist Teil des Programms und nicht als regionale Beschränkung zu verstehen. Wir – auch Teilnehmer, die nicht aus dem Rheinland stammen, sind herzlich eingeladen – wollen keine graue und leblose Security-Konferenz in einem der typischen Tagungshotels mit Strafvollzugszellen abhalten, sondern uns in einem lockeren Ambiente treffen

Zu der Premiere erwarten wir u.a. die beiden Dipl. Psychologen und Marktforscher Ankha Haucke und Udo Eichstädt, die die „Entsicherung am Arbeitsplatz" erforscht haben. Sie werden über die (bezeichnende) Atmosphäre in den zweistündigen Tiefeninterviews berichten, uns einen Teil der Ergebnisse präsentieren und diese mit uns diskutieren. Außerdem wollen wir von Ihnen wissen, ob wir Sie auch nach der Premiere zu weiteren Stammtischen begrüßen dürfen, was Sie sich von zukünftigen Stammtischen erwarten und u.U. anders machen würden.

WÖLFE & GEISSEN - Der Rheinische Security-Stammtisch. Köln, Di., 14. November 2006 ab 18.30 h (Vortrag Eichstädt/Haucke ab 19.15 h). **Teilnahmebeitrag:** Euro 15,00. **Anmeldung:** sense@known-sense.de. **Organi-**

Newsletter Nr. 5 erscheint im Januar 2007.

Awareness-Klassiker Virusquartett

Zwei Jahre nach der Erstauflage unseres Awareness-Klassikers erscheint im November 2006 die neue, überarbeitete Version des Virusquartetts, „Computerluder – Das Virusquartett 2.0" mit neuen Kategorien und neuen Viren und Würmern. Partner ist IIR Technology, der Veranstalter des IT-Security-Forums 2006 in Bad Homburg (27.-30.11.2006).

Spiegel online schrieb 2004: »... Lehrreich: Es gibt dämliche Werbegags und es gibt wirklich intelligente. Computerluder, das wohl weltweit erste Virenquartett, gehört fraglos zur letzteren Kategorie (...) Auf 32 »Blatt« lernt man die »Leistungsdaten« und Charakteristika von acht Virengruppen - und das macht mehr Laune als in der Realität...« Und das ZDF berichtete: »... Statt mit langweiligen Autos (...) kann man hier mit (...) Computerviren punkten und die mieslichen-fieslichen Übertäter näher kennen lernen.« Weitere Clippings: »...Gefahrlos Zocken (...) Das Quartettspiel »Computerluder« erlaubt nun den gefahrlosen Umgang mit den digitalen Plagegeistern...« (manager-magazin). »Was Marken nützt: Meine Dönerbude , mein Virusquartett... ...« (brand eins). »Lerne Deinen Feind kennen – Wer sich lieber von einem Spiel als von einem Computervirus infizieren lässt, für den hat die Kölner Agentur known_sense (...) ein witziges Spiel entwickelt ...« (Kölner Stadtanzeiger).

Am 29. November stellt Dietmar Pokoyski die Studie „Entsicherung am Arbeitplatz" im Rahmen des IT-Security-Forum 2006 in Bad Homburg vor. Die Forum-Teilnehmer erhalten über den Partner IIR das Virusquartett 2.0. ■