

Tagung „Der Mensch im Sicherheitskonzept“

Sicherheits- statt Risikofaktor

von Dr. Johannes Wiele

26. Februar 2008

Der „Faktor Mensch“ hat in der Informationssicherheit einen deutlich positiveren Wert, als es die aktuelle Diskussion ahnen lässt. Dies stellten die Referenten auf einer spannenden SIMEDIA-Tagung in Frankfurt fest. Auch praktische Anleitungen zur Einbindung von Mitarbeitern in Sicherheitsmaßnahmen fehlten nicht.



Viel Interesse, aber oft auch großes Staunen: Der Umgang mit dem „Faktor Mensch“ in der Informationssicherheit war für manche Besucher der Simedia-Tagung noch aufregendes Neuland.
Foto: Simedia

Die IT-Sicherheit behandelt den Menschen primär als Risikofaktor. „Muss man ihn nicht als Sicherheitsfaktor bezeichnen?“, fragten gleich mehrere Vorträge der Tagung „Der Mensch im Sicherheitskonzept“ am 16. Januar in Frankfurt. Je komplexer ein System werde, desto hilfloser sei die Sicherheitstechnik und desto wichtiger werde der Sicherheitsbeitrag des Menschen.

Für diesen Aspekt allerdings sind viele Spezialisten blind. „Es gibt unzählige Statistiken, die den Anteil an menschlichen Fehlleistungen bei Luftfahrtunfällen bestimmen“, berichtete etwa Rolf P. Schatzmann von Pricewaterhouse-Coopers Zürich, „aber keine darüber, wie viele Unfälle allein durch richtige Entscheidungen der Piloten und Lotsen verhindert wurden.“

In der IT-Sicherheit sei der Beitrag der Mitarbeiter ähnlich wertvoll. Er könne überdies durch Verhaltenscodizes gefördert werden – Unternehmen,

die sich ethische Richtlinien auf die Fahnen schrieben, könnten auf signifikant weniger Fälle von Wirtschaftskriminalität verweisen. Ein weiterer wirksamer Faktor sei ein gutes Unternehmensklima.

Schatzmann warf einen kritischen Blick auf die technische Kontrolle von Arbeitnehmern, die er primär bei Vorgesetzten verortete, die von ihren Mitarbeitern abhängig sind und den Leistungen nicht trauen. Er plädierte aber auch dafür, Kontrolle zur Voraussetzung von Vertrauen zu machen. Damit allerdings führte er nicht nur das Prinzip Vertrauen logisch ad absurdum, sondern opferte überdies den ökonomischen Vorteil, den vertrauenswürdige Umgebungen durch die Ablösung teurer Kontrollmechanismen bieten können. Dennoch machte gerade Schatzmanns sachlicher Vortrag Mut, in Maßnahmen zur Motivation der Mitarbeiter zu investieren.

Rainer von zur Mühlen vom BDSI und Almuth Wünsch von Incognito zeigten, wie schwierig es ist, für Kampagnen die Akzeptanz der Mitarbeiter zu erlangen. „Kann man sicheres Verhalten nicht einfach fordern?“, fragte sich das Publikum. Die Referenten aber waren sich einig: Mitarbeit an der Sicherheit erreicht man nicht durch Anweisungen. Almuth Wünsch wies zusätzlich darauf hin, dass Regeln in Unternehmen oft gar nicht konsequent umgesetzt werden könnten. Oft schaffe man Sicherheits-Policies, verlange aber zugleich, dass Mitarbeiter sie für wichtige Kunden außer Kraft setzten. Solche Unstimmigkeiten müssten in jedem Unternehmen offen angesprochen werden, damit man trotzdem zu einem vernünftigen Risikoverhalten gelangen könnte, forderten die Referenten.

Ronald Hauber von Daimler zeigte, wie sich Audits positiv auf den menschlichen Beitrag für die Informationssicherheit auswirken können, wenn man sie als Service für die überprüften Abteilungen gestaltet und ihren Missbrauch für Machtspiele unterbindet. Dietmar Pokoyski von Known Sense widmete sich dem Thema Sicherheitskultur und warnte davor, Mitarbeiter wie Kinder mit Tricks „erziehen“ zu wollen: „Das durchschauen Erwachsene sofort“. Security-Managern befänden sich „zwischen der Position eines Doppelagenten und der eines Seelsorgers“ und müssten selbst tiefenpsychologische Grundsätze berücksichtigen – so solle man es ernst nehmen, dass Mitarbeiter Sicherheitshilfsmittel wie etwa Kennwörter gern mit Persönlichem verknüpfen. Hier nähert sich Pokoyski dem Autor unseres Kennwort-Tipps auf Seite 70/71, der die Verwendung der Namen von Haustieren und Familienmitgliedern als Passwörter ins Positive wendet.

Weitere Vorträge befassten sich mit Maßnahmen gegen die Drift zwischen Theorie und Praxis in existierenden Sicherheitsumgebungen (Cuno Künzler), dem Spannungsfeld Mensch-Technik (Beate Kallenbach-Herbert), der Wirkungskontrolle von Awareness-Kampagnen (Konrad Zerr) und einer konkreten Kampagne bei DuMont Schauberg (Jürgen Grüne und Eva Leuer).

Pressekontakt SIMEDIA:

Marcus Nebel
Tel. 0228 - 96 29 3 -74
Fax 0228 - 96 29 3 -90
Email: ne@simedia.de
www.simedia.de