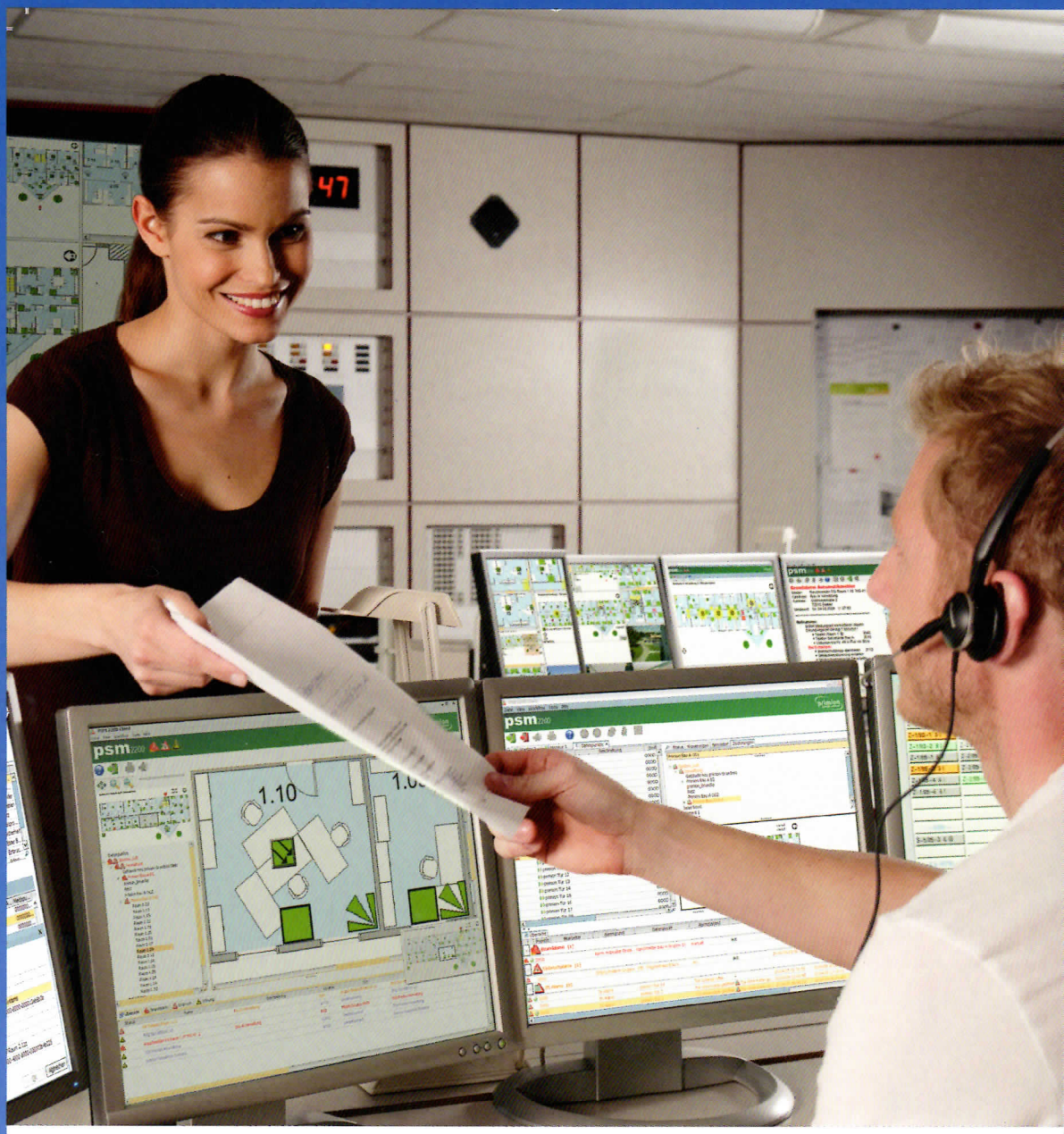
77500 · ISSN 1866-2420
Einzelverkaufspreis: 12,- €

September/Oktober 5/2012



SECURITY insight

Fachzeitschrift für Unternehmenssicherheit



www.security-insight.com

Jenseits von Wissen und Wollen

Security Awareness als steuerbare Komponente der Unternehmenskultur

Von Michael Helisch

War Sicherheit vor Jahren noch ein kaum wahrnehmenbares Thema, so hat es mittlerweile seinen Platz in der öffentlichen Diskussion gefunden. Davon sollten auch betriebliche Sicherheitsaktivitäten profitieren. Doch trotz zum Teil umfangreicher Security-Awareness-Aktivitäten ist die gelebte (Sicherheits-) Realität in Unternehmen eine andere. Behandeln wir mit dem bisherigen Vorgehen lediglich die Symptome, ohne die Ursachen des Problems zu beseitigen?

Es gibt mittlerweile eine Vielzahl handwerklich sehr guter Awareness-Kampagnen und -Programme. Methodisch aber gehen die meisten am Ziel vorbei, da die Maßnahmen im Wesentlichen aus zwei „Heilmitteln" bestehen: Vermittlung von sicherheitsrelevantem Wissen (Schulung) und Marketing für das Thema Sicherheit. Keine Frage, beides ist unabdingbar für das Gelingen eines Awareness-Vorhabens. Aber sie alleine führen nicht zur gewünschten Verhaltensänderung respektive dauerhaften Umsetzung von Sicherheits-Richtlinien im beruflichen Alltag. Denn Wissen (Schulung) und Wollen (Marketing) können lediglich die Spitze des Eisbergs verändern, nicht aber den großen Teil unter der Wasseroberfläche. Wer Awareness-Maßnahmen plant und umsetzt, kommt nicht umhin, unter die Wasseroberfläche zu schauen und sich zu fragen, welches „Klima" dort herrscht, denn dieses „Klima" hat wesentlichen Einfluss auf Größe und Form des gesamten Eisbergs. Übertragen auf Security-Awareness

ruft dies folgende Fragen auf: Welchen Einfluss haben soziale und organisationsspezifische Faktoren auf sicherheitskonformes Verhalten und wie wirken sie? Wie nutzen wir entsprechende Erkenntnisse, um Awareness-Aktivitäten effektiver, effizienter und nachhaltiger zu machen?

Unternehmens- und Sicherheitskultur

Bei den sozialen und organisationsspezifischen Einflussfaktoren geht es in erster Linie um die Unternehmens- und Sicherheitskultur. Wie aktuelle Studien zeigen, stellt der Umgang damit im Kontext von Sensibilisierungsmaßnahmen eine enorme Herausforderung für die Sicherheits-Verantwortlichen dar. Über 50 Prozent der Studienteilnehmer beziehen unternehmenskulturelle Besonderheiten nicht in Planung und Umsetzung von Awareness-Maßnahmen ein – mit negativer Konsequenz für deren Nachhaltigkeit.

Sicherheit ist, sofern entsprechend gelebt, stets ein Teilaspekt der Unternehmenskultur. Ob sie zu einer eigenen Subkultur wird, entscheidet der Einzelfall. Wichtig ist, dass Sicherheit keine Gegenkultur zur Unternehmenskultur wird, vielmehr müssen sie sich ergänzen und zueinander passen. Beispiele für die Kollision beider Kulturen liefern die verschiedenen Ansatzmöglichkeiten von „Social Engineering". Diese Methode ist gerade deshalb so erfolgreich, weil sie menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität bewusst ausnutzt, um Menschen zu manipulieren und sie zu Handlungen zu bewegen, die der Sicherheit abträglich

Foto: Edler von Rabenstein - Fotolia.com

Bis den Mitarbeitern ein Licht in Sachen Unternehmenssicherheit aufgeht, kann es mitunter eine Weile dauern. Das liegt aber nicht an ihnen, sondern an der oft mangelnden Awareness-Kompetenz von Geschäftsleitung und Sicherheits-Verantwortlichen.

sind. In einer Unternehmenskultur, die – überspitzt formuliert – nach dem Prinzip „Befehl und Gehorsam" funktioniert, wird ein Social Engineer, der sich der Technik „massiver Druckaufbau" bedient, leichter ans Ziel kommen als in einem Umfeld, in dem ein konstruktiver Diskurs üblich ist.

Ein anderes Beispiel ist das Sperren des Computers bei Abwesenheit: Möglicherweise kommen die Mitarbeiter dieser Anforderung nach, weil sie erkannt haben, dass sie sinnvoll ist. Sie tun es vielleicht aber auch deshalb, weil es in ihrer Bezugsgruppe (zum Beispiel das Team) Usus ist. Der Einzelne verhält sich teamkonform und vermeidet so abfällige Kommentare der Teammitglieder, wenn er den PC nicht sperrt.

„Gegenseitige Wertschätzung" findet sich als im- oder expliziter Wert bei vielen Unternehmen und zeigt sich auch darin, den Kollegen, ob bekannt oder unbekannt, wie selbstverständlich die Tür aufzuhalten. Unternehmen, in denen es schon als ungebührlich angesehen wird, nach der Zutrittsberechtigung überhaupt zu fragen, haben ein Sicherheitsproblem. Wie geht man damit um, wenn man die Sicherheit erhöhen will? Wird die „gegenseitige Wertschätzung" aus dem Wertekanon entfernt? Sicher nicht. Gefragt ist hier vielmehr eine schnelle, unternehmensweite und eindeutige Thematisierung des Umgangs mit diesem Wert.

Auf der anderen Seite gibt es Unternehmenskulturen mit vergleichsweise starker Sicherheitskultur. So liegt die Vermutung nahe, dass sich beispielsweise Mitarbeiter eines Herstellers von Süßwaren in punkto Sicherheit anders verhalten als die Belegschaft eines Rüstungskonzerns. Das bedeutet aber nicht, dass sich im letztgenannten Umfeld Sicherheitsmaßnahmen leichter implementieren lassen. Die entscheidende Frage ist auch hier: Inwieweit passen die Awareness-Aktivitäten und der damit möglicherweise

SI-Autor Michael Helisch ist Inhaber der Firma HECOM Security Awareness Consulting (www.hecom-consulting.de), die sich auf die Sensibilisierung des Sicherheitsfaktors Mensch spezialisiert hat. Zudem ist er Initiator der Studienreihe „Security Awareness in der betrieblichen Praxis" und hat 2009 zusammen mit Dietmar Pokoyski das erste deutsche Praxishandbuch zum Thema Security Awareness herausgegeben.

einhergehende Veränderungsbedarf zur vorhandenen Unternehmenskultur?

Corporate Identity als Katalysator für gelebte Sicherheit

Awareness-Aktivitäten zu planen und umzusetzen, ohne sich die Frage zu stellen, wie es um die Corporate Identity bestellt ist, bedeutet nicht nur, wesentliche Erfolgsfaktoren für sicherheitskonformes Verhalten von vornherein auszuklammern, sondern letzten Endes auch, Ressourcen zu vergeuden. Warum? Die Corporate Identity bildet nach Ansicht des Wirtschaftswissenschaftlers Heribert Meffert die strategische Klammer, die gleichermaßen nach innen wie nach außen wirkt mit dem Ziel, einen optimalen Gesamteffekt für das Unternehmen zu erreichen. Sie bestimmt das Verhalten der Organisationsmitglieder (Corporate Behaviour), die Art, wie sich das Unternehmen darstellt (Corporate Design), seine Kommunikationsprozesse (Corporate Communcations) sowie die Unternehmenskultur (Corporate Culture).

Es liegt auf der Hand, dass Mitarbeiter, die sich in hohem Maße mit dem eigenen Unternehmen identifizieren, auch eine starke emotionale Bindung an das Unternehmen haben. Loyale Mitarbeiter schützen das Unternehmen jederzeit auch ohne externe Anreize – das reduziert die Notwendigkeit von „Marketingmaßnahmen" deutlich. Zudem ist die Bereitschaft, sich Wissen anzueignen, mit dem das Unternehmen aktiv geschützt werden kann, eine ganz andere als bei Mitarbeitern mit geringer oder gar fehlender emotionaler Bindung an das Unternehmen. Sie werden nur das Allernötigste tun oder sich gar destruktiv verhalten.

Fazit

Wer Awareness-Maßnahmen implementieren will, muss sicherheitsrelevantes Wissen adäquat vermitteln und die Mitarbeiter via „Marketing" dazu bringen, den Inhalt der Policies umsetzen zu wollen. Bildlich gesprochen ist man damit lediglich bei der Pflicht, also der Umsetzungs*absicht*, die Kür in Form der *tatsächlichen Umsetzung* sicherheitsrelevanter Verhaltensvorgaben ist damit noch nicht abgelegt. Wirklich erfolgreich und nachhaltig wirken Awareness-Maßnahmen erst, wenn der Aspekt „Organisation" systematisch einbezogen wird. Damit können organisationsbedingte Stolpersteine, die die Verhaltensumsetzung behindern, identifiziert und aus dem Weg geräumt werden. Eine „gesunde" Organisation wirkt aus der Perspektive des einzelnen Organisationsmitglieds *per se* als Motivator für „Compliance" jeglicher Art. Dies macht allerdings eine Sichtweise auf das Thema Sicherheit erforderlich, die weit über „klassisches Sicherheitsdenken" hinausgeht. Denn Sicherheit wird von dem, was im Unternehmen täglich passiert, massiv beeinflusst und wirkt gleichzeitig darauf ein.

Sowohl Awareness als auch Sicherheit sind somit nicht etwas „Eigenes", sondern lebendiger Teil des Gesamtsystems

Unternehmen. Will man also nicht nur Symptome behandeln, sondern vielmehr die Ursachen sicherheitsinkonformen Verhaltens aufdecken und bekämpfen, sollte möglichst umfassend und aus verschiedenen Blickwinkeln hinter die Kulissen menschlichen Handelns im Unternehmen geschaut werden. Das bedeutet auch, dass bei Awareness-Aktivitäten Fragen zum Beispiel zu Mitarbeiterloyalität und -zufriedenheit, gelebter Führung, Vertrauen und Verantwortung, Kommunikation, Konflikt- und Problemmanagement untersucht und beantwortet werden. Security-Awareness ist damit stets auch ein Stück weit Unternehmensentwicklung, von der nicht nur die Sicherheit, sondern das Unternehmen als Ganzes profitiert.

Brisante Sicherheitsthemen am Comer See

Lange nichts gehört von der Mafia. Na gut, hin und wieder eine Schießerei wie in den Morgenstunden des 15. August 2007 in Duisburg. Auch haben wir uns daran gewöhnt, dass der Begriff im Zusammenhang mit dem Namen Berlusconi immer mal wieder fällt. Ansonsten aber ist die Organisierte Kriminalität italienischer Prägung doch eher was für spannende Kinoabende als für die Sicherheitsarbeit in Unternehmen.

Diese Wahrnehmung mag zwar ein wenig am konspirativen Charakter der kriminellen Machenschaften liegen. Aber das ist kurzsichtig gedacht, wie man auf der jüngsten Führungskräftetagung des Verbands für Sicherheit in der Wirtschaft Baden-Württemberg (VSW BW) erfuhr. Die in Venedig lebende deutsche Journalistin Petra Reski schilderte anschaulich, wie sich die Mafia seit 40 Jahren in Deutschland gut eingerichtet hat und wie dies von deutschen Politikern, der Gesetzgebung und zum Teil auch von den Sicherheitsbehörden ignoriert wird. Die Mafia hat hier zu Lande großen Einfluss auf Politik und Wirtschaft. Vor dem Hintergrund riesiger Bauprojekte, beispielsweise „Stuttgart 21", schilderte sie ihre Befürchtung, dass die Mafia durch Korruption und andere Delikte noch tiefer in unsere Wirtschaft eindringt und den fairen Wettbewerb immer mehr behindert.

Das Mafia-Thema lag auf der Hand, denn die Führungskräftetagung fand diesmal im sonnigen Italien statt, was nicht nur von einem glücklichen Händchen von VSW-BW-Geschäftsführer Karl Stefan Schotzko in Sachen *location* zeugte, sondern auch für ein gutes Gespür für Sicherheitsthemen, die trotz hoher Brisanz viel zu selten auf der Agenda stehen. Rund 50 Führungskräfte aus den verschiedensten Bereichen der Sicherheit hatten sich zum Wissens-Update und Networking hoch über dem Comer See im internationalen Konferenzzentrum „Villa La Collina" der Konrad-Adenauer-Stiftung getroffen und lauschten den Vorträgen. Diese reichten von der deutschen Sicherheitslage (Axel Mögelin, Stabsbereichsleiter des baden-württembergischen Landeskriminalamts) über „Human Branding" für Sicherheits-Verantwortliche (Jon Christoph Berndt, brandamazing), „Return on Security Invest" (Michael Zoratti, SecureLINE) und Haftungsrisiken für Manager im Sicherheitsgewerbe (Rechtsanwalt Dr. Martin Wesch) bis hin zum unvermeidlichen Cybercrime (Volker Birk, Chaos Computer Club). Und für alles zusammen spannte Prof. Dr. Günther Schmid vom Bundesnachrichtendienst den globalen Bogen in einem gewohnt niederprasselnden Informationsgewitter.

Insgesamt eine wieder informative und hochkarätig besetzte Veranstaltung, für die sich die weite Anreise sicherlich für alle Teilnehmer gelohnt hat. Für das kommende Jahr lud VSW-BW-Präsident Wolfgang Geyer bereits jetzt für den 10. bis 12. Juli nach Dresden ein.

IK

WWW.VSW-BW.COM