

# Security Awareness 2.0 – der Weg zu aktiv gelebter Sicherheitskultur

**Unternehmen betreiben oft eine physische «Sicherheitsaufrüstung» und schotten sich mit allen ihnen zur Verfügung stehenden Sicherheitswerkzeugen ab. Die meisten Massnahmen reglementieren dabei den Mitarbeitern den Netzzugang. Die effizienteste und einfachste Möglichkeit – die direkte und positive Kommunikation zum Thema und die persönliche Ansprache zu den Mitarbeitern – erfolgt mit niedriger Priorität und kommt dementsprechend viel zu kurz.**

VON MARCUS BEYER

**M**it dem Übergang von der industriellen zur Wissensgesellschaft stellen Wissen und Innovation zunehmend die zentralen Objekte der Wertschöpfung dar. Wissen ist längst zum vierten Produktionsfaktor geworden. Jedoch: kein Wissen ohne Informationen. Information ist unabdingbare Ressource im Leistungserstellungsprozess, gleichsam wesentlicher Faktor für erfolgreiches unternehmerisches Handeln. Sie ist die Basis für unternehmerische Entscheidungsprozesse, denn ohne Information keine (sinnvolle) Entscheidung. Informationen sind zugleich ein wesentlicher Wettbewerbsfaktor.

## Wissen als zu sichernder «Wert» im Unternehmen

Um Informationssicherheitskultur in Unternehmen und Verwaltung nachhaltig zu etablieren, werden viele organisatorische Massnahmen ergriffen. Unternehmen müssen mit dem Paradox leben, dass der Mensch nicht nur den grössten Risikofaktor darstellt, sondern gleichzeitig auch den wichtigsten Wert für das Unternehmen.

Hier besteht bis dato immer noch substanzieller Nachholbedarf. Zwar ist zu beobachten, dass man in jüngster Zeit häufiger bereit ist, dem Thema Gehör zu schenken, dennoch: Der Mensch wird in der betrieblichen Realität als Sicherheitsfaktor leider (noch) zu häufig vernachlässigt. Die relevanten Elemente der viel zitierten Sicherheitskette sind also nicht stabil genug. In der Konsequenz bedeutet dies, dass ein ganzheitliches, die relevanten Risikofaktoren integrierendes Sicherheitsmanagement in

der Praxis eher die Ausnahme als die Regel darstellt.

## Wachsamkeit; stärker als Überwachung

Neben Wachsamkeit im Unternehmen, dem gesunden Misstrauen und dem nachhaltigen Einsatz von Sicherheitsrichtlinien, ist angesichts der aktuellen Entwicklung der Sicher-

heitsbedrohungen ein weiterer Begriff von immenser Bedeutung bei der Bekämpfung von Internet-Kriminalität: die Sensibilisierung. Wird berücksichtigt, dass in 80% aller Sicherheitsvorfälle der Mensch und nur in 20% die Technik versagt hat, kann man schnell ein ungenutztes Sicherheitspotenzial bei den Mitarbeitern feststellen.

Vielen Unternehmen fehlt aber eine gelebte Sicherheits- und Präventionskultur. Je nachdem, welches Verhalten der Mitarbeiter im Umgang mit der IT-Infrastruktur und damit mit seinen eigenen oder den Informationen des Unternehmens an den Tag legt, wird er zu einem Risikofaktor oder einem entscheidenden Instrument zur Risikominimierung. Der Mensch spielt als «Risikofaktor» im Sicherheitskontext eine zentrale Rolle. Hier muss die Verhaltensänderung beginnen, eben der Aufbau einer unbewussten Kompetenz, das Ziel und nicht die blosser Vermittlung von Wissen. Letzteres führt nur für einen kurzzeitigen Moment zu einer Steigerung des Sicherheitsbewusstseins – ist aber nicht nachhaltig im Kopf und dem Verhalten der Mitarbeiter verankert.

## Security Awareness – von Menschen für Menschen

Awareness ist von Menschen für Menschen gemacht. Da menschliches Verhalten nicht «programmierbar» ist, müssen die beeinflussenden Faktoren mitberücksichtigt werden. Das macht Awareness schnell zu einem komplexen Vorhaben.

Damit Awareness-Aktivitäten eine realistische Chance auf Erfolg haben, muss man als Verantwortlicher für derartige Aktivitäten wissen, welche grundsätzlichen Beeinflussungsfaktoren wirken, welche Folgen diese Faktoren haben und wie sie zusammenwirken. Um mit dieser Komplexität sinnvoll umgehen zu können bzw. sie auf ein praktikables Mass zu reduzieren, muss beurteilt werden können, welche dieser Faktoren im

Fortsetzung auf Seite 48

## SecurityConference'09

### SICHERHEIT – COMPLIANCE – KOSTENSENKUNG

Die «SecurityConference'09» vom 10. September 2009 ist eine Plattform für Wissens- und Informationsaustausch für ganzheitliche Informations- und Informatik-sicherheit. Sie richtet sich an Verwaltungsräte, Geschäftsführer und Inhaber, an CEOs, CIOs, CSOs, CTOs sowie Sicherheitsbeauftragte, Security-Architekten, Riskmanager und Security Experts und Projektleiter für Sicherheit in Unternehmen und Organisationen. Organisiert wird die SecurityConference'09 vom Bassersdorfer Unternehmen für Informationssicherheit, Ispin AG.

Persönlichkeiten aus Wirtschaft, Politik, Forschung und Technologie sprechen über Themen, Trends und Antworten für zukunftsweisende und praktikable Schritte in eine verbesserte Informations- und IT-Sicherheit: Ulrich Tilgner, Gerold Bühler, Horst Teltschik, Thomas Lüscher, Peter Fischer, Hanspeter Thür, Stephan Klapproth, Heinrich Müller, Dieter Meier. Referate-Themen sind u.a.:

■ Wirtschaftspolitische Herausforderungen in einer globalen Krise. Gerold Bühler, Präsident EconomieSuisse



■ Von Gorbatschow bis Medwedew – die Strategie für eine gesamteuropäische Sicherheit. Prof. Dr. h.c. Horst Teltschik, langjähriger ehemaliger Leiter Münchner Konferenz für Sicherheitspolitik

■ Das Zusammenspiel von Organen – Risikomanagement am Menschen. Prof. Dr. med. Thomas F. Lüscher, Professor & Chairman, Klinik für Kardiologie, Herz-Kreislauf-Zentrum, Universitätsspital Zürich

■ USA, Iran, Afghanistan: Gelingt ein Politwechsel? Ulrich Tilgner, Korrespondent und Buchautor

■ MELANI als wichtige Säule zum Schutz der nationalen Informationsinfrastrukturen. Peter Fischer, Informatikstrategieorgan des Bundes  
Die SecurityConference'09 findet am 10. September 2009 von 8 bis 18 Uhr im X-TRA, Limmatstrasse 118, 8031 Zürich statt ([www.x-tra.ch](http://www.x-tra.ch)). Teilnahmegebühr: CHF 680.– exkl. MWST. Mitglieder von Verbänden erhalten 10 Prozent Rabatt. Weitere Informationen: Markus Kaegi, Tel. 044 838 31 11, [markus.kaegi@SecurityConference.ch](mailto:markus.kaegi@SecurityConference.ch), [www.SecurityConference.ch](http://www.SecurityConference.ch)



**Führungskräfte müssen den  
sicheren Umgang mit sensiblen  
Daten aktiv vorleben.**

Bild: René Sputh – www.fotolia.com

#### Fortsetzung von Seite 46

organisatorischen Umfeld des Unternehmens wichtig, respektive welche weniger wichtig sind. Ein Awareness-Projekt umsetzen ist damit ein Prozess aus Wissen – Abgleichen – Entscheiden – Umsetzen.

#### Mitarbeitende: wichtiger Teil der «Sicherheitskette»

Awareness macht einerseits Arbeit, andererseits ist der «return on security invest» im Kontext Awareness mangels eindeutiger Messbarkeit nur schwerlich nachweisbar. Was also tun? Einfach so weitermachen wie bisher? Abwarten, bis etwas passiert, in der Hoffnung, dass nichts passiert? Falls etwas passiert, einfach den Ursachen auf den Grund gehen und daran arbeiten? Warum, so die berechtigte Frage, sollte man sich den mit Awareness verbundenen Aufwand freiwillig aufhalsen? Die Antwort darauf ist relativ einfach: Wo der Mensch intervenierend in sicherheitsrelevante Prozesse und Arbeitsabläufe einwirkt, ist er automatisch Teil der «Sicherheitskette». Dabei muss jedes Glied dieser Kette stark sein, sonst wird sie den ihr zugeordneten Zweck, Sicherheit zu gewährleisten, nicht erfüllen können. Wer also ein nachhaltiges Risiko- bzw. Sicherheitsmanagement anstrebt, der kommt an dem Einbeziehen des Menschen nicht vorbei.

#### Positives Vorleben ist effektiver als reaktive Nachsorge

Der Aufbau einer Informationssicherheitskultur ist dann erfolgreich, wenn die Führungskräfte im Unternehmen den Umgang mit sensiblen Daten und der IT gewissenhaft vorleben. Diese Vorbildfunktion ist ein

entscheidender Punkt im Aufbau und in der Pflege der Informationssicherheit. Den Führungsstab frühzeitig mit einzubeziehen, entscheidet über den Erfolg der Awareness-Massnahme und deren Umsetzung. Dabei ist allerdings darauf zu achten, dass diese keine reine Aufgabe der Informatik ist und bleibt. Die Sicherheitskultur muss abteilungsübergreifend gedacht, geführt und geprägt werden.

Die Sensibilisierung von Mitarbeitern und die damit verbundenen Massnahmen oder die Security-Awareness-Kampagne als solche, führen dabei oftmals nicht nur zu einer Kulturveränderung, sondern sie fordern auch Organisationsanpassungen; in- und ausserhalb von Unternehmung und Verwaltung. Wenn Mitarbeiter während des Awareness-Programms im Positiven «proviziert» und zum Handeln angeregt

**«Security Awareness 2.0 ist ein aktiver Veränderungsprozess. Ein sicheres Verhalten entsteht nur in Verbindung eines bewussten Agierens der Mitarbeiter. Das muss im Unternehmen zukünftig – am besten jetzt und sofort – zu einem existenziellen Kompetenzfaktor werden.»**

werden, bekommen IT- und Organisationseinheiten viel zu tun – denn hier wird Awareness pure Realität. Auf jede Massnahme muss auch eine Umsetzung erfolgen, und wenn Mitarbeiter sensibilisiert werden, dann werden Sie aktiv! Security Awareness ist also Umsetzung pur.

#### Der «Faktor Mensch»

Sich mit dem «Faktor Mensch» intensiv auseinanderzusetzen bedeutet, mögliche Auswirkungen des Verhaltens der Mitarbeiter besser einzuschätzen und das Bedrohungspotenzial einzuschränken. Das heisst, dass Unternehmen ihre Sicherheitsprogramme nicht nur auf die technologische Sicht begrenzen dürfen. Sie müssen vielmehr lernen zu verstehen, wie Menschen «ticken» und mit Daten, Informationen und Unternehmenswerten umgehen. So werden sie in der Lage sein, ihre Netzwerke nicht nur vor externen Eindringlingen zu schützen, sondern auch davor, dass Nutzer, wie etwa Mitarbeiter, vertrauensvolle Daten versehentlich oder wohl wissend an Dritte weitergeben.

Was braucht der Mitarbeiter, um seine Einstellung, seine Werthaltung und somit seine Kulturäusserung zugunsten der Unternehmenssicherheit zu verändern, oder gar zu verbessern? Im Sport finden wir Spielregeln. Diese verhindern, dass jede Handlung subjektiv anders verstanden wird. Was heisst «fair»? Was verstehen Mitarbeiter unter «Vertrauen»? Sollen Kulturmassnahmen greifen, so braucht ein Unternehmen Spielregeln. Zudem muss es wissen, was Menschen brauchen, um diese umzusetzen. Die Kenntnisse über Wertvorstellungen und Kulturen sind entscheidend für das Sicherheitsleben, um Foul-Spiele zu erahnen und um über die verschiedenen Lernkurven Verbesserungen einzubringen.

#### Oldschool Awareness vs. Awareness 2.0?

Hier kommt in Abgrenzung zur «Oldschool» der Ansatz der «Awareness 2.0» ins Spiel, der sich im Wissen um die dynamischen, prozessorientierten Komponenten von Awareness-Massnahmen (Change-Management-Prozess) von den reinen didaktischen bzw. ausschliesslich marketinggesteuerten Massnahmen, die vor allem auf die klassische Lerntheorie und

Betriebswirtschafts- bzw. Organisationslehre setzen, unterscheidet. Die Trennung ist vor allem methodischer Art, denn das Wissen um (respektive die Nutzung von) Oldschool bildet eine Basis von Awareness 2.0, die sich aber eben nicht nur mit Vorträgen, Trainings, Postern & Co. zufrieden gibt.

Awareness 2.0 orientiert sich konsequent an

- Blended Learning,
- klassischem und innovativem Marketing,
- integrierter und systemischer Kommunikation (intern wie auch interkulturell),
- psychologischen Grundlagen und
- Change Management.

Last but not least sind für eine nutzbringende Umsetzung von Awareness Ausdauer und Konsequenz unabdingbar. Awareness ist keine blossе Aneinanderreihung von Einzelaktionen, sondern ein langfristiger Prozess, mitunter auch ein langfristiger Prozess der Unternehmensentwicklung mit offenem Ausgang.

#### Bewährte Ansätze nutzen

Awareness 2.0 stellt also nicht nur den Menschen in den Mittelpunkt ihrer Betrachtung, sondern nutzt Methoden, die über eine grösstmögliche Passung zum Gegenstand ihrer Betrachtung, dem Menschen, verfügen. Awareness 2.0 heisst: State-of-the-art-Ansätze für kommunikative Massnahmen zu nutzen, die sich bereits in anderen Kontexten und Kanälen bewährt haben. Heisst auch, das Bewusstsein dafür zu entwickeln, dass z.B. die Struktur von Kampagnen nicht zwingend modular (bzw. in Blöcke) eingeteilt werden muss. Und es bedeutet, dass eine Kampagne nicht nur aus einem Comic und der maximalen Diversifizierbarkeit hinsichtlich der Verwertung seiner Figuren bis hin zum Tassenaufdruck besteht. ■■■■

**Marcus Beyer** ist Architect Security Awareness bei der ISPIN AG. Durch seine geisteswissenschaftliche Ausbildung ist sein Blick auf die Organisation, den aktiv agierenden Mitarbeiter als Individuum und die Kommunikation im Unternehmen gerichtet – die Grundlage für eine gelebte Informationssicherheit im Unternehmen. Er erarbeitet, plant und organisiert Security-Awareness-Kampagnen für und in Unternehmen der Schweiz und in Deutschland.