

# Der Weg zur gelebten Sicherheitskultur

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. Marcus Beyer



**Marcus Beyer**  
ist Architect Security  
Awareness bei der  
ISPIN AG  
marcus.beyer@ispin.ch

Um Informationssicherheitskultur in Unternehmen und Verwaltung nachhaltig zu etablieren, werden viele organisatorische Massnahmen ergriffen. Unternehmen betreiben dabei oft eine physische «Sicherheitsaufrüstung» und schotten sich mit allen ihnen zur Verfügung stehenden Sicherheitswerkzeugen ab. Die meisten Massnahmen reglementieren dabei den Mitarbeitern den Netzzugang, sehr schnell spricht man bei Nichteinhaltung von gesetzten Regeln Mahnungen oder gar Kündigungen aus. Die effizienteste und eigentlich einfachste Möglichkeit, nämlich die direkte und positive Kommunikation zum Thema und die persönliche Ansprache zu den Mitarbeitern, hat wenig Priorität und kommt dementsprechend viel zu kurz.

## **Wissen ist ein zu sichernder Wert im Unternehmen**

Mit dem Übergang von der Industrie- zur Wissensgesellschaft stellen Wissen und Innovation zunehmend die zentralen Objekte der Wertschöpfung dar. Wissen ist längst zum vierten Produktionsfaktor geworden. Jedoch gilt: Kein Wissen ohne Informationen, denn diese sind unabdingbare Ressourcen im Leistungserstellungsprozess und gleichsam wesentlicher Faktor für erfolgreiches unternehmerisches Handeln. Informationen sind die Basis für unternehmerische Entscheidungsprozesse, denn ohne sie gibt es keine (sinnvollen) Entscheidungen. Informationen sind zugleich ein wesentlicher Wettbewerbsfaktor.

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 jüngerer Zeit häufiger bereit ist, dem Thema Gehör zu schenken, dennoch wird der Mensch im betrieblichen Alltag als Sicher- ▶

heitsfaktor 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 ist stärker als Überwachung**

Neben Wachsamkeit im Unternehmen, dem gesunden Misstrauen und dem nachhaltigen Einsatz von Sicherheitsrichtlinien ist angesichts der aktuellen Entwicklung der Sicherheitsbedrohungen ein weiterer Begriff von immenser Bedeutung bei der Bekämpfung von Internetkriminalität: die Sensibilisierung. Wird berücksichtigt, dass in 80 Prozent aller Sicherheitsvorfälle der Mensch und nur in 20 Prozent 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 bloße Vermittlung von Wissen. Letzteres führt nur für einen kurzzeitigen Moment zu einer Steigerung des Sicherheitsbewusstsein – 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, beziehungsweise sie auf ein praktikables Mass zu reduzieren, muss beurteilt werden können, welche dieser Faktoren im organisatorischen Umfeld des Unternehmens wichtig, respektive welche weniger wichtig sind. Ein Awareness-Projekt umsetzen ist damit ein Prozess aus Wissen, Abgleichen, Entscheiden und Umsetzen.

### **Mitarbeitende sind 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 aufhalten? 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 zgedachten Zweck, Sicherheit zu gewährleisten, nicht erfüllen können. Wer also ein nachhaltiges Risiko- beziehungsweise 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 innerhalb und ausserhalb von Unternehmen und Verwaltung. Wenn Mitarbeiter während des Awareness-Programms im Positiven «provoziert» und zum Handeln angeregt 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

«Security Awareness 2.0 ist ein aktiver Veränderungsprozess und muss zu einem existenziellen Kompetenzfaktor werden.»

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 Foulspiele zu erahnen und um über die verschiedenen Lernkurven Verbesserungen einzubringen. Sensibilisierungsmassnahmen auf dem Weg zum sicheren Unternehmen sind wie PR-Massnahmen auf dem Weg zum starken Image. Sie sind unumgänglich! Solange der PR-Verantwortlicher nicht versteht, weshalb gute PR für das Unternehmen wichtig ist, werden PR-Massnahmen nie gut ankommen.

### Old School Awareness versus Awareness 2.0

Hier kommt in Abgrenzung zur «Old School» der Ansatz des «Awareness 2.0» ins Spiel, der sich im Wissen um die dynamische, prozessorientierten Komponenten von Awareness-Massnahmen (Change-Management-Prozess) von den reinen didaktischen respektive ausschliesslich marketing-gesteuerten Massnahmen unterscheidet, die vor allem auf die klassische Lerntheorie und Betriebswirtschafts- beziehungsweise Organisationslehre setzen. Die Trennung ist vor allem methodischer Art, denn das Wissen um (respektive die

Nutzung von) «Old School» 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, klassischen und innovativem Marketing, integrierter und systemischer Kommunikation (intern wie auch interkulturell), psychologischen Grundlagen und Change Management.

### Awareness ist ein langfristiger Prozess

Last but not least sind für eine nutzbringende Umsetzung von Awareness Ausdauer und Konsequenz unabdingbar. Awareness ist keine blosser Aneinanderreihung von Einzelaktionen, sondern ein langfristiger Prozess, mitunter auch ein langfristiger Prozess der Unternehmensentwicklung mit offenem Ausgang. 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, den 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 und das Bewusstsein dafür zu entwickeln, dass zum Beispiel die Struktur von Kampagnen nicht zwingend modular 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. ■

Anzeige



## Der Netzguide – Sichern Sie sich Ihren Informationsvorsprung.

Der Netzguide ist das Kompendium für ICT-Entscheider in der Schweiz. Mit Fachkompetenz und Praxisbezug schreiben Autorinnen und Autoren aus der Schweizer ICT-Branche über aktuelle Trends. Der Netzguide bietet Ihnen somit eine solide Werbepattform für Inserate, Cases und Firmenporträts.

Nutzen auch Sie jetzt diese Gelegenheit, Patrick Brazzale berät Sie gern.

E-Mail: [patrick.brazzale@netzmedien.ch](mailto:patrick.brazzale@netzmedien.ch), Tel. 061 366 63 29

Weitere Informationen finden Sie unter [www.netzguide.ch](http://www.netzguide.ch)

netzwoche

Das Schweizer ICT-Magazin  
für Business-Entscheider