LANline Spezial

€ 9,–

IV/2007

konradin MEDIENGRUPPE

Das Magazin für Netze, Daten- und Telekommunikation

www.lanline.de

Security- und Compliance-Guide

Mit Marktübersicht Content-Security-Lösungen

Konzepte, Ideen und der menschliche Faktor
Awareness, Spionage, Identitätsmanagement

Richtlinienkonformer IT-Betrieb
Risikomanagement, Forensik, IT-Audits

Sicherheitstechnik
Single Sign-on, Network Access Control

Einflüsse auf das sicherheitsbezogene Verhalten

Awareness-Arbeit und Unternehmenskultur

Die Bedeutung des Faktors Mensch innerhalb der Diskussionen um Informationssicherheit hat sich deutlich gewandelt. Hatte die menschliche Komponente bis Mitte der neunziger Jahre allein den Touch des „größten anzunehmenden Risikos", kommt der kritische Betrachter mittlerweile nicht mehr umhin, den Menschen mit in ganzheitliche Sicherheitsüberlegungen einzubeziehen und ihm neben risiko- auch sicherheitsfördernde Aspekte zuzuschreiben.

Menschliches Handeln im unternehmerischen Alltag vollzieht sich in einem dynamischen Kontext. Es wird durch vielfältige Rahmenbedingungen, Anforderungen, Aufgaben und Ziele beeinflusst, die in den seltensten Fällen alle unter einen Hut zu bringen sind. Auch sind wir nicht nur einigen wenigen Aufgaben, Anforderungen und Zielen verpflichtet. Besser bekannt ist uns das Gefühl, im beruflichen Alltag vor der schieren Anzahl der Aufgaben, Anforderungen und Ziele, die an uns herangetragen werden, „in die Knie zu gehen". Dass der eine oder andere Aspekt dabei einfach verloren geht, erscheint mehr als verständlich. An oberster Stelle der Prioritätenskala steht üblicherweise das Erreichen der Geschäftsziele, für das jeder Mitarbeiter idealerweise im Rahmen definierter Prozesse einen mittelbaren oder unmittelbaren Beitrag leistet. Sicherheitsbezogenes Verhalten wird dabei beeinflusst durch Vorgaben, die im Rahmen der Sicherheitsarchitektur sowie im Rahmen sicherheitsrelevanter Strategien und Prozesse festgelegt sind. Art und Umfang der implementierten Sicherheitstechnik und -infrastruktur bestimmen, ob Sicherheit automatisch und gleichsam „unsichtbar" im Hintergrund abläuft und inwieweit dem Anwender auch eine aktive Rolle zukommt. Die Bandbreite der bearbeiteten Sicherheitsthemen ist unternehmensindividuell verschieden und hängt insbesondere von der Unternehmensgröße und den vorhandenen finanziellen Mitteln für Sicherheit ab.

Ob und in welchem Ausmaß Sicherheit gelebt wird, hängt neben dem grundsätzlichen Stellenwert, den Sicherheit im Unternehmen hat, sowohl vom Kulturkreis als auch von der Unternehmenskultur ab. Dass der jeweilige kulturelle Hintergrund auch zu Verhaltensunterschieden im beruflichen Kontext führt, ist nahe liegend. Wer würde beispielsweise einem Spanier seine geliebte Siesta abspenstig machen wollen? Das Führungs- und Entscheidungsverhalten in japanischen Unternehmen wird sich bei aller Vielfalt der Unternehmen in zentralen Punkten signifikant von dem in deutschen Unternehmen unterscheiden.

Warum sind Onlinehilfen in Softwareanwendungen für asiatische Länder anders aufgebaut und stärker in das Produkt integriert als bei uns? Weil der Gebrauch eines Handbuchs dort einem Gesichtsverlust gleichkommt – der Nutzer würde dann als unfähig gelten [1].

Den Zusammenhang zwischen kulturellen Unterschieden und der grundsätzlichen Einstellung zu Sicherheit stellt unter anderem Geert Hofstede in seinen Publikati-

onen her. Kultur ist seiner Ansicht nach „die mentale Programmierung, die die Mitglieder einer Gruppe oder Kategorie von Menschen von einer anderen unterscheidet und die jedes Mitglied einer gegebenen Gemeinschaft, Organisation oder Gruppe erlebt und entsprechend derer er/sie voraussichtlich folgerichtig handeln wird“ [2]. Als einen von fünf Faktoren zur Beschreibung unterschiedlicher Kulturen verwendet er den Begriff der „Uncertainty Avoidance“. In Ländern mit niedriger Unsicherheitsvermeidung (zum Beispiel Schweden und Dänemark) wird die Tatsache, dass die Wirkungen der eigenen Handlungen in Vergangenheit und Zukunft nicht vollständig voraussehbar sind, eher akzeptiert. Derartige Kulturen gelten als tolerant. Stark unsicherheitsvermeidende Kulturen (wie etwa Griechenland, Portugal oder Argentinien) sind bestrebt, das Gefühl von Sicherheit über Technologie, Gesetze und Religion herzustellen [3].

Damit sind diese Kulturen nicht per se „sicherer“. Hofstedes Aussagen geben aber einen Hinweis auf die Frage, welcher grundsätzliche Ansatz auf dem Weg zu „mehr Sicherheit“ für welchen Kulturkreis geeignet oder weniger geeignet ist.

Dieser Frage kommt im unternehmerischen Kontext Bedeutung zu, insbesondere in multinationalen Unternehmen. So wird der Versuch, die in der schwedischen Unternehmenszentrale erfolgreiche Security-Awareness-Kampagne auch in der brasilianischen Niederlassung umzusetzen, erhebliche Reibungsverluste erzeugen, im schlimmsten Falle ganz auf Ablehnung stoßen. Dies lässt sich leicht vermeiden, indem kulturelle Unterschiede bei der Umsetzung eines Security-Awareness-Programms erkannt und berücksichtigt werden.

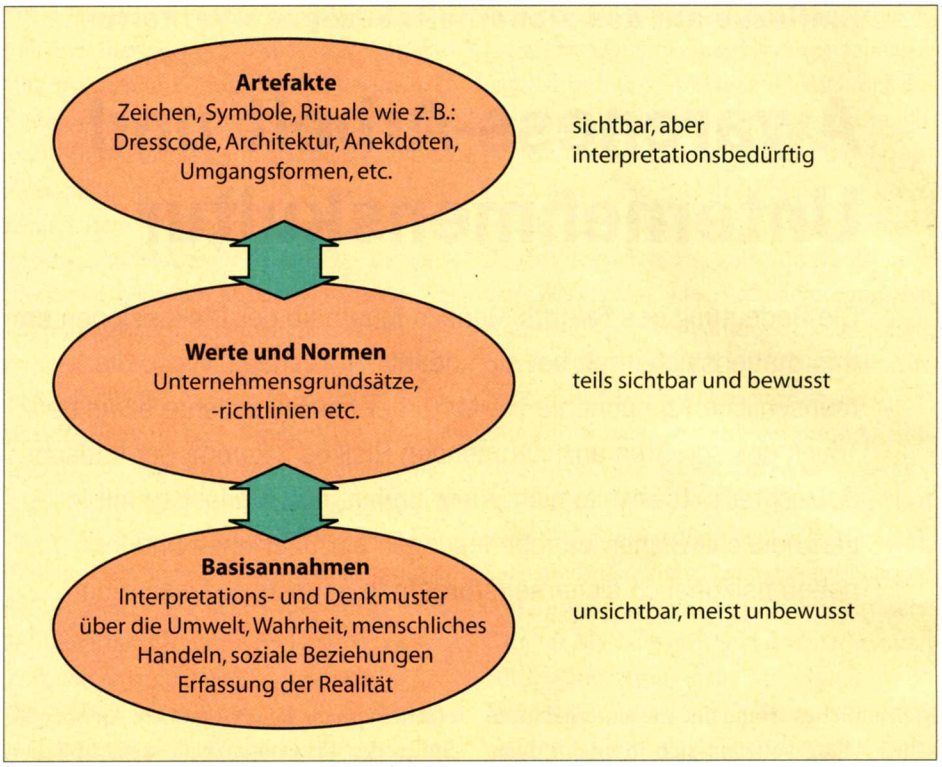

Bild 2. Die drei Ebenen der Organisationskultur nach Schein [5]

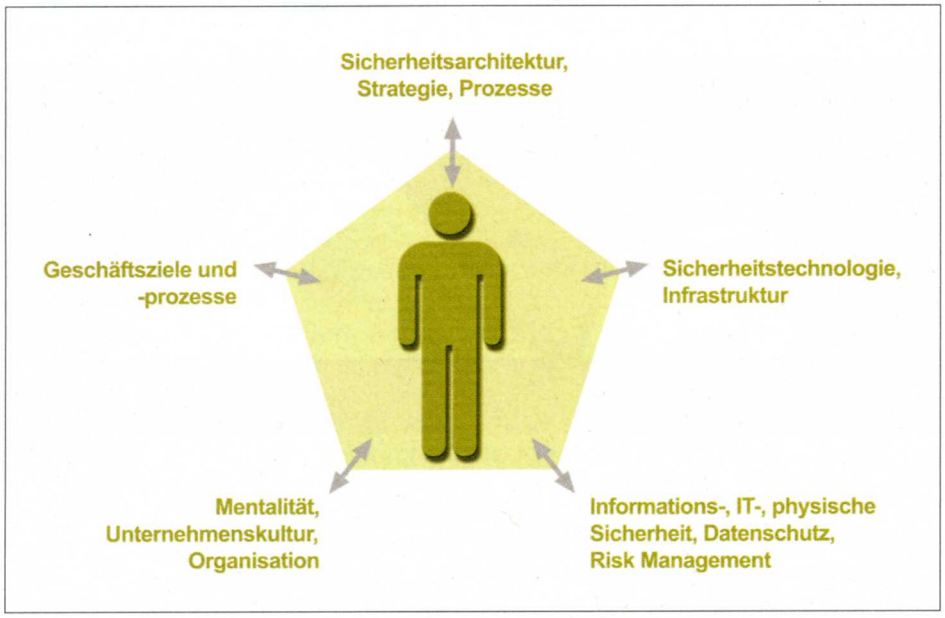

Bild 1. Sicherheitskonformes Verhalten ist eine mehrdimensionale und ganzheitliche Aufgabe, in deren Mittelpunkt der Mensch steht

Gibt es „die“ Unternehmenskultur?

Um es gleich vorweg zu nehmen: Nein, eine eindeutige und allgemein gültige Definition von Unternehmenskultur wird man vergeblich suchen. Dennoch lässt sich Unternehmenskultur anhand einiger weniger Merkmale beschreiben. Sie ist ein kollektives Phänomen, das Ideen, Vorstellungen und Werte bezeichnet, die die Organisationsmitglieder gemeinsam verfolgen, für gewöhnlich ohne sich dies bewusst zu machen. Bei aller Individualität der einzelnen Mitarbeiter erzeugt Unternehmenskultur ein gewisses Maß an Einheitlichkeit, den „Unternehmenscharakter“. Die Unternehmenskultur ist eine im Wesentlichen unsichtbare Einflussgröße. Damit gemeint sind alle indirekten Orientierungsmuster und Handlungen, mit denen man ein akzeptiertes Mitglied des Unternehmens wird oder ist. Unternehmenskultur bestimmt, welche Handlungsweisen erwünscht und welche unerwünscht sind. Ihr liegt ein „stiller“, das heißt nicht systematisch vermittelter, dafür aber weit verzweigter „Lernplan“ zugrunde, der von Mitarbeitergeneration zu -generation weitergereicht wird. Unternehmenskultur ist damit auch Unternehmenshistorie [4].

Mitarbeiter für das Thema Sicherheit zu sensibilisieren, um langfristig sicherheitskonformes Verhalten zu erreichen, stellt je nach Unternehmen einen unterschiedlich starken Eingriff in die gewachsene Unternehmenskultur dar. Ob darin Konfliktpotenzial enthalten ist, hängt davon ab, ob und inwieweit sich die Mittel und Maßnahmen, die im Verlauf einer Awareness-Kampagne zum Einsatz kommen, mit den unternehmensindividuellen Artefakten, Werten und Normen sowie Basisannahmen in Einklang bringen lassen. Selbiges gilt es auch bei den Anforderungen zu beachten, die Mitarbeitern in Bezug auf sicherheitskonformes Verhalten abverlangt werden.

Unternehmenskultur und Sicherheit

Insbesondere die Basisannahmen bleiben langfristig konstant, da sie kaum hinterfragt werden. Durch gezielte Maßnahmen sind sie nur schwer zu beeinflussen. Andererseits ist Unternehmenskultur kein völlig statisches Gebilde. Sie prägt zwar das Verhalten der Organisationsmitglieder, gleichzeitig beeinflusst das Verhalten der Organisationsmitglieder aber auch die Unternehmenskultur, vor allem durch diejenigen (neuen) Verhaltensweisen, die sich im Zeitablauf bewähren haben. Auf den Punkt gebracht bedeutet dies: Unternehmenskultur und sicherheitsbezogene Gestaltungsmaßnahmen beeinflussen sich gegenseitig. Ob dies aus der Perspektive der Unternehmenssicherheit positiv zu beurteilen ist, hängt von der Stärke der Unternehmenskultur und deren Inhalten im Einzelnen ab.

Besonders vielfältige Beispiele, bei denen Sicherheit mit Kultur oder der Unternehmenskultur kollidiert, liefern die 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 Mitarbeiter zu manipulieren und sie zu Handlungen zu bewegen, die die Sicherheit gefährden. Halten Sie sich nur einmal vor Augen, wie oft Sie schon Ihnen unbekannte Personen, die sich vermeintlich ziellos über die Gänge Ihres Unternehmens bewegen, daraufhin angesprochen haben, wen oder was diese Person sucht.

Genauso existieren Unternehmenskulturen, bei denen sicherheitskonformes Denken und Handeln einen vergleichsweise hohen Stellenwert haben. So werden Mitarbeiter eines Herstellers von Süßwaren eine andere Einstellung zu Sicherheit haben

als die Belegschaft eines Rüstungskonzern, wo sich Sicherheitsmaßnahmen wesentlich leichter implementieren lassen.

Anpassung oder Konfrontation ?

Diese Frage möchte ich mit einem klaren „jein" beantworten. Sensibilisierung für Sicherheit geht immer einher mit einem Eingriff in die Unternehmenskultur. Die Frage ist nur, wie tief die Eingriffe in die beschriebenen Ebenen der Organisationskultur sind. Rüttelt man an den Grundfesten einer Organisation, wird man sich schwertun, Mitarbeiter zur Umsetzung sicherheitskonformen Verhaltens zu motivieren.

Ziel: Aufmerksamkeit bei den Mitarbeitern

Will man Sicherheit nachhaltig – das heißt nicht nur „per Ordre de Mufti" – erhöhen, kommt man nicht umhin, Sicherheit „an den Mann und an die Frau zu bringen". Dies bedeutet, bewusst Aufmerksamkeit zu schaffen und Interesse zu wecken, denn schließlich sollen die Kolleginnen und Kollegen zu sicherheitskonformem Verhalten motiviert (und nicht gezwungen) werden. Sicherheit mit System an die Mitarbeiter zu verkaufen, ist daher nicht „anrüchig", sondern sinnvoll. Dies bedeutet aber, dass Sensibilisierungsmaßnahmen an bewusst gewählten Stellen vom unternehmenskulturellen „Mainstream" wie zum Beispiel dem gängigen visuellen Erscheinungsbild eines Unternehmens abweichen müssen, um überhaupt wahrgenommen zu werden. Das bewusste Spiel mit unternehmenskultureller Konformität und Non-Konformität von Security-Awareness-Projekten ist meiner Ansicht nach ein Erfolg versprechender Ansatz. Angesichts der Tatsache, dass es dafür aber kein „Kochrezept" gibt, ist es umso wichtiger, dass die Projektbeteiligten das entsprechende Feingefühl besitzen, was im Hinblick auf das Erreichen der Ziele aus Sicherheitssicht sinnvoll ist, respektive der Unternehmenskultur (noch) zugemutet werden kann.

Fazit

Dass sich Unternehmenskultur und Sicherheit wechselseitig beeinflussen, liegt auf der Hand. Bestimmte Unternehmenskulturen begünstigen per se ein vergleichsweise stärker ausgeprägtes Sicherheitsniveau. Sicherheitsanforderungen wiederum üben mittel- bis langfristig auch einen Anpassungsdruck auf die Unternehmenskultur aus. Den einzig richtigen Weg des Zusammenspiels zwischen sicherheitsfördernden Sensibilisierungsmaßnahmen und der Unternehmenskultur wird es nicht geben – den für das einzelne Unternehmen richtigen hingegen schon.

Michael Helisch/wj

Michael Helisch ist Gründer und Inhaber von Hecom Security Awareness Consulting in München.

Quellen

[1] Michael Reiter, Der Mensch ist das Maß. Computer Zeitung, 11.02.1999, Seite. 8.
[2] Geert Hofstede, Interkulturelle Zusammenarbeit. Kulturen – Organisationen – Management, Wiesbaden 1993, Seite 5.
[3] Geert Hofstede und Gert Jan Hofstede, Cultures and Organizations: Software of the Mind, New York, 2. Auflage 2005, Seite 168 f.
[4] Georg Schreyögg, Diagnose der Unternehmenskultur (Begleittext zum Video der Fernuniversität Hagen), 1989, Zusammenfassung B. K.
[5] Edgar H. Schein, Organizational Culture and Leadership, San Francisco 1985

Weitere Literatur:

Erich Frese, Grundlagen der Organisation. Konzept – Prinzipien – Strukturen, Wiesbaden, 7. Auflage 1998 und 8. Auflage 2000.
Erich Frese, Grundlagen der Organisation. Entscheidungsorientiertes Konzept der Organisationsgestaltung, Wiesbaden, 9. Auflage 2005.