PSW GROUP
SSL-Zertifikate
bereits ab 15 € pro Jahr
Vertrauen Sie auf über 10 Jahre Erfahrung
Ausstellung in nur 10 Min. nach erfolgreicher Prüfung Ihres Auftrags inkl. kostenlosem deutschen Support
www.psw.net

Hakin9 extra

HARD CORE IT SECURITY MAGAZINE

Hakin9 EXTRA Ausgabe 1/2012

Linux Memory Forensics

Datenmissbrauch und die „Privatisierung" der IT

Security Awareness – Ursachenbekämpfung statt Kurieren an Symptomen

Online-Lotterien

Security Awareness – Ursachenbekämpfung statt Kurieren an Symptomen

Michael Helisch

War Sicherheit vor geraumer Zeit Jahren noch ein kaum wahrnehmenbares Thema, so hat Sicherheit Dank Social Media und Co. mittlerweile seinen Platz in der öffentlichen Diskussion gefunden – von dieser Entwicklung sollten grundsätzlich auch betriebliche Sicherheitsaktivitäten profitieren. Doch die gelebte (Sicherheits-) Realität in Unternehmen ist eine andere. Warum profitieren betriebliche Security Awareness Aktivitäten nicht wirklich von der gestiegenen Sensitivität in der breiten Öffentlichkeit?

IN DIESEM ARTIKEL ERFAHREN SIE…

- Welchen Einfluss soziale bzw. organisationsspezifische Faktoren auf securitykonformes Verhalten haben und wie sie wirken
- Mehr über „Unternehmenskultur" und „Corporate Indentity" sowie deren Auswirkungen auf die gelebte Unternehmenssicherheit
- Wie man Security Awareness Aktivitäten mehr Effektivität und Nachhaltigkeit verleiht

WAS SIE VORHER WISSEN SOLLTEN…

- Kein spezielles Vorwissen

Kurieren wir mit dem bisherigen Vorgehen in Sachen Awareness lediglich an Symptomen, ohne die Ursachen des Problems anzugehen?

Wenn man die immer zahlreicher werdenden Aktivitäten zur Sensibilisierung von Mitarbeitern und Führungskräften analysiert, wird man feststellen, dass mittlerweile eine Vielzahl handwerklich sehr gut gemachter Security Awareness Kampagnen und Programme auszumachen ist. Methodisch aber gehen die meisten dieser Kampagnen am Ziel vorbei, da die im Rahmen der Kampagnen vorgesehenen Awareness-Maßnahmen im Wesentlichen aus zwei „Heilmittel" bestehen: Zum einen Vermittlung bzw. Schulung von sicherheitsrelevantem Wissen, zum anderen Marketing für das Thema Sicherheit. Keine Frage, Wissensvermittlung und „Sicherheitsmarketing" sind unabingbar für das Gelingen eines Awareness Vorhabens. Allein diese beiden methodischen Hilfsmittel einzusetzen, wird aber nicht zu der möglichst umfassenden und dauerhaften Umsetzung von Sicherheitsrichtlinien im beruflichen Alltag führen. Warum nicht? Weil Wissen(-svermittlung) & Wollen (Sicherheitsmarketing) lediglich die Spitze des Eisbergs verändern können, nicht aber jenen Teil, der sich unter der Wasseroberfläche befindet und dessen überwiegende Masse ausmacht. Wer Security 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 hervor: Welchen Einfluss haben soziale bzw. organisationsspezifische Faktoren auf securitykonformes Verhalten und wie wirken sie? Was genau ist damit eigentlich gemeint? Wie nutzen wir entsprechende Erkenntnisse, um Awareness Aktivitäten effektiver, effizienter und nachhaltiger zu machen?

Unternehmens- und Sicherheitskultur

Bei den sozialen bzw. organisationsspezifischen Einflussfaktoren securitykonformen Verhaltens geht es in erster Linie um die Faktoren Unternehmens- und Sicherheitskultur. Wie die Studie „Security Awareness in der betrieblichen Praxis" (Helisch 2009 und 2011) gezeigt hat, stellt der Umgang mit diesen beiden Faktoren im Kontext von Sensibilisierungsmaßnahmen eine enorme Herausforderung für die Verantwortlichen von Security Awareness Aktivitäten dar. Über 50% der Studienteilnehmer beziehen unternehmenskulturelle Besonderheiten nicht in die Planung und Umsetzung von Awareness-Maßnahmen ein – mit entsprechender Konsequenz für die Nachhaltigkeit solcher Maßnahmen.

Ob und in welchem Ausmaß Sicherheit gelebt wird, hängt neben dem grundsätzlichen Stellenwert, den Si-

cherheit im Unternehmen hat, sowohl vom Kulturkreis als auch von der Unternehmenskultur ab. Dass der jeweilige kulturelle Hintergrund auch zu Verhaltensunterschieden im beruflichen Zusammenhang führt, ist nahe liegend. Verbunden mit der Konsequenz, dass Awareness-Maßnahmen in international agierenden Unternehmen immer auf nationale oder gar lokale Besonderheiten überprüft werden müssen, die dann bei Bedarf in die jeweilige Kampagne einzubauen sind. Die Umsetzung einer Awareness-Kampagne nach den Gießkannenprinzip, d.h. gleichermaßen über alle Tochtergesellschaften eines Unternehmens hinweg, mag vielleicht weniger Aufwand und Kosten generieren, sie wird, so umgesetzt, aber am eigentlichen Ziel vorbei führen oder das Ziel gar konterkarieren.

Gelebte Unternehmenskultur macht den Unterschied – im Kontext Sicherheit genauso wie bezogen auf die Frage, was ein Unternehmen langfristig am Markt erfolgreich macht. Unternehmenskultur lässt sich anhand einiger weniger Merkmale beschreiben (Schreyögg und Koch 2007).

- Sie ist ein kollektives Phänomen, das eine gemeinsame Orientierung hinsichtlich Ideen, Vorstellungen, Werten und Handlungsmustern beschreibt und die die Organisationsmitglieder gemeinsam verfolgen, ohne sich dies wirklich bewusst zu machen.
- Bei aller Individualität der einzelnen Mitarbeiter erzeugt Unternehmenskultur ein gewisses Maß an Einheitlichkeit, den „Unternehmenscharakter".
- Unternehmenskultur ist eine im Wesentlichen unsichtbare Einflussgröße. Damit gemeint sind alle indirekten Orientierungsmuster und Handlungen, mit denen man akzeptiertes Mitglied des Unternehmens wird oder ist.
- Unternehmenskultur gibt den Organisationsmitgliedern Muster vor, anhand derer das Erlebte interpretiert werden kann.
- Unternehmenskultur geht über bewusste Denk- und Erkenntnisprozesse hinaus. Wesentlich ist ihr emotionaler Charakter.
- Unternehmenskultur bestimmt, welche Handlungsweisen erwünscht und welche unerwünscht sind.
- Unternehmenskultur liegt ein „stiller" d.h. nicht systematisch vermittelter dafür aber weit verzweigter historischer „Lernprozess" zugrunde der von Mitarbeiter-Generation zu Generation weitergereicht wird. Damit ist Unternehmenskultur ein dynamischer, nie endender Prozess.

Mitarbeiter für das Thema Sicherheit zu sensibilisieren, um langfristig sicherheitskonformes Verhalten zu erreichen, stellt einen Eingriff in die gewachsene Unternehmenskultur dar, da jeder einzelne Mitarbeiter sein Verhalten in bestimmten, sicherheitsrelevanten Situationen ändern soll. Dies wird nicht ohne Auswirkungen auf das Gesamtsystem Unternehmen bleiben, denn die via Securitypolicy eingeforderten Verhaltensänderungen vollziehen sich im Kontext einer, wie auch immer gelebten Unternehmenskultur. Inwieweit darin Konfliktpotential enthalten ist, hängt davon ab, wie gravierend die durch Sicherheit getriggerte Änderungen auf die aktuelle Unternehmenskultur wirken und wie stark oder schwach die Unternehmenskultur ausgeprägt ist.

Auf welchen Ebenen manifestiert sich Unternehmenskultur? Zuoberst die sichtbare Ebene der Artefakte. Darunter die Ebene der Werte und Normen, die nur zum Teil sichtbar und bewusst ist, sowie die unsichtbare, unbewusste Ebene der Basisannahmen (siehe Abbildung, angelehnt an Schein 1985).

Kulturwandel im eigentlichen Sinne ist dann gegeben, wenn sich die Basisannahmen verändern. Hinsichtlich der Mechanismen, die zu einer Veränderung der Basisannahmen führen sind primäre Faktoren (z.B. charismatische Ausstrahlung des Vorgesetzten oder des Geschäftsführers) und sekundäre (z.B. formalisierte Regelungen) zu unterscheiden. Die sekundären entfalten dabei ihre kulturwandelnde Wirkung nur dann, wenn sie im Einklang mit den primären stehen (Frese 2000). Das bedeutet in der Konsequenz: Das Vorleben von Verhaltensmaximen, insbesondere durch die Führungskraft, ist von entscheidender Bedeutung und wichtiger als das, was schriftlich fixiert oder mittels Rege-

Abbildung 1. *Der Mensch, das zentrale Bindeglied zwischen Sicherheitstechnik und -prozessen*

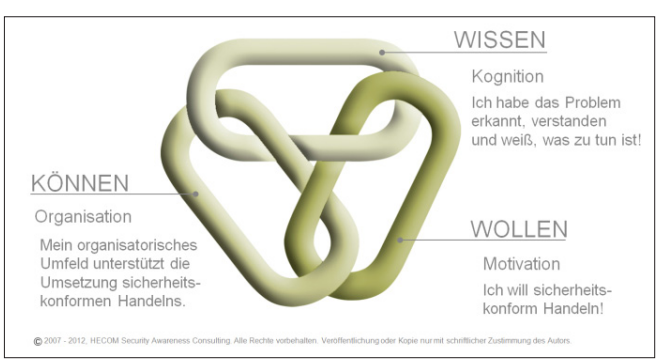


Abbildung 2. *Security Awareness – mehr als nur „Wissen" und „Wollen"*

lungen bzw. Gestaltung von Systemen angestrebt wird (Schein 1985). Auf den Punkt gebracht bedeutet dies: Unternehmenskultur und sicherheitsbezogene Gestaltungsmaßnahmen beeinflussen sich gegenseitig.

Sicherheitskultur in der betrieblichen Praxis

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. Sicherheits- und Unternehmenskultur müssen sich ergänzen bzw. zueinander passen.

Besonders vielfältige Beispiele, bei denen Sicherheit mit Kultur bzw. Unternehmenskultur kollidiert, liefern die verschiedenen Ansatzmöglichkeiten von Social Engineering. Diese Methode ist gerade deshalb so erfolgreich, weil sie menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität bewusst ausnutzt, um Mitarbeiter zu manipulieren und sie zu Handlungen zu bewegen, die der Sicherheit abträglich 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 an sein Ziel kommen, als in einem Umfeld, in dem ein konstruktiver Diskurs gelebt wird. Die Frage, wie mit Sicherheitsvorfällen umgegangen wird, findet seine unternehmenskulturelle Entsprechung in der Frage, welcher Umgang mit Problemen in meinem unternehmerischen Umfeld üblich ist. Werden sie eher „unter den Teppich gekehrt“ oder werden sie als Herausforderungen angesehen, denen man sich ohne Vorbehalte stellt? Im erstgenannten Umfeld wird bspw. die unternehmensinterne Anlaufstelle für sog. Wistleblowing, also dem Aufdecken von Misständen und Handelungen, die gegen das Gesetz oder grundlegende Unternehmenleitlinien verstossen, nicht wirklich häufig von den Mitarbeitern kontaktiert bzw. mit entsprechenden Informationen versorgt werden.

Beispiel Sperren des Computers beim Verlassen des Arbeitsplatzes. Möglicherweise komme ich dieser Sicherheitsanforderung nach, weil ich erkannt habe, dass es Sinn macht. Ich tue es vielleicht aber gerade deshalb, weil es in der Bezugsgruppe, derer ich mich zugehörig fühle (z.B. mein Team), Usus ist, den Computer beim Verlassen des Arbeitsplatzes zu sperren. Ich als

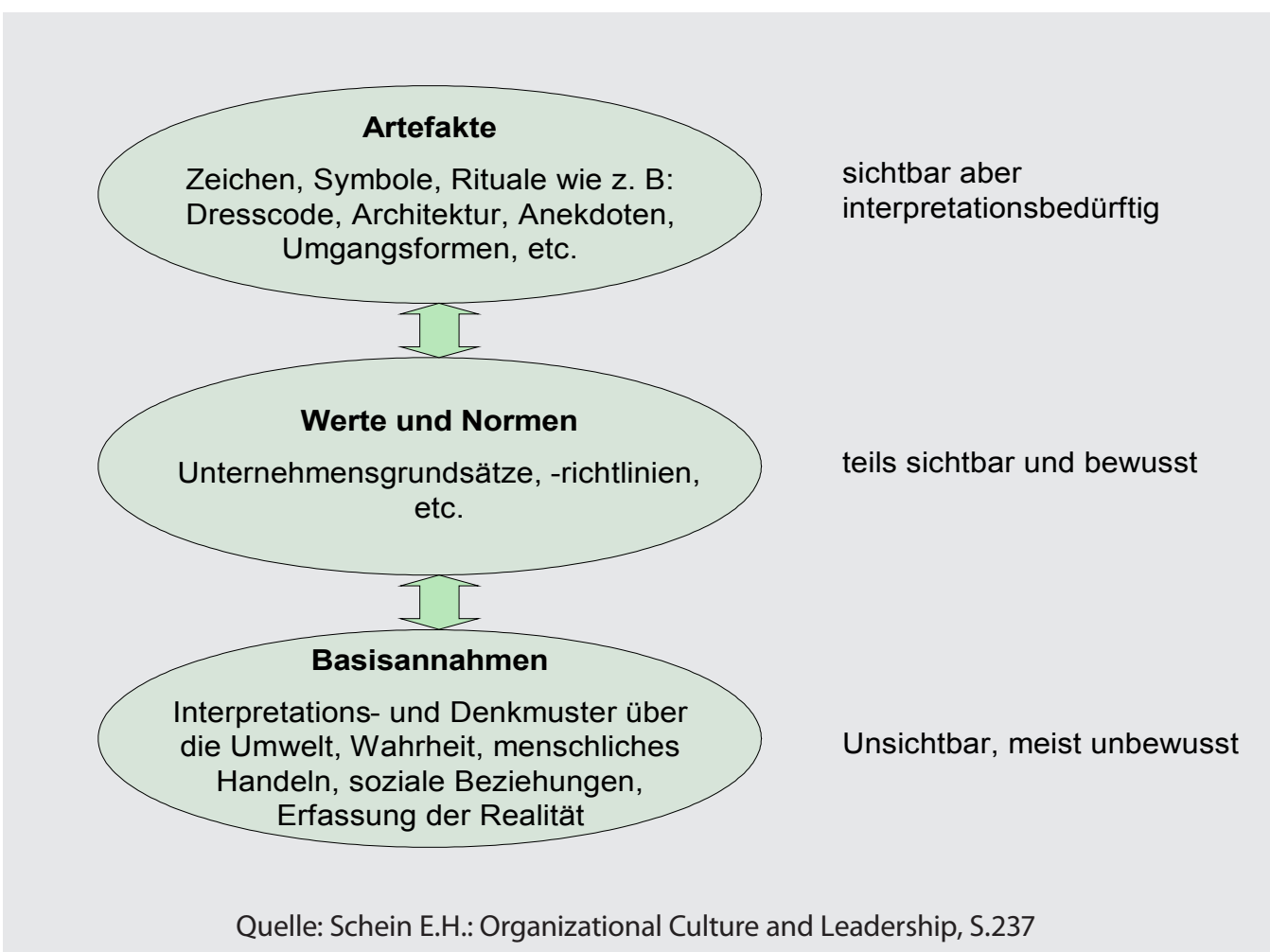


Abbildung 3. *Die drei Ebenen der Unternehmenskultur*

einzelner verhalte mich teamkonform und vermeide so abfällige Kommentare der Teammitglieder.

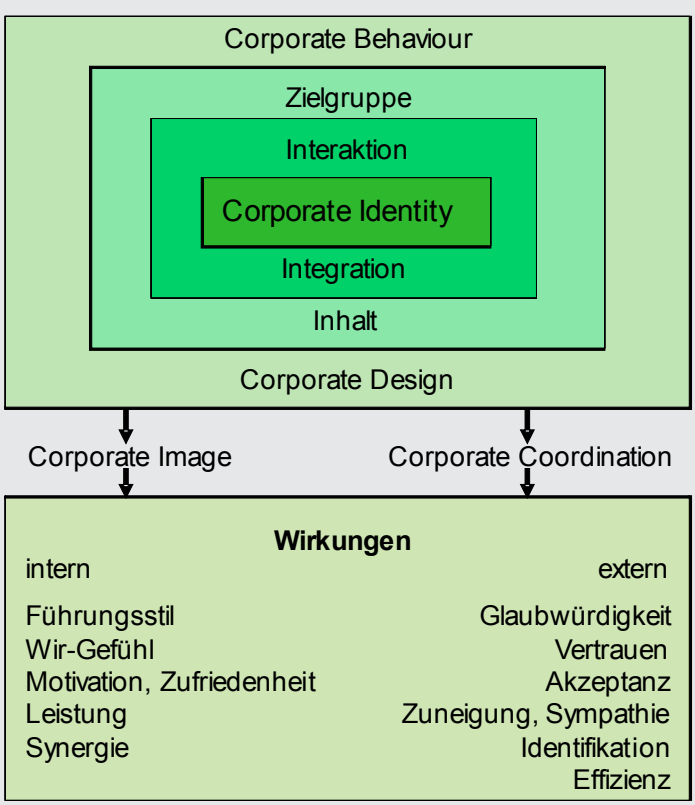
„Gegenseitige Wertschätzung“ findet sich als im- oder expliziter Wert bei vielen Unternehmen und zeigt sich u.a. darin, dass den Kollegen, ob bekannt oder unbekannt, wie selbstverständlich die Tür aufgehalten wird. Unternehmen, in denen schon das Nachfragen bzgl. der Zutrittsberechtigung als etwas angesehen wird, das „sich nicht gehört“, haben ein Sicherheitsproblem. Wie geht man damit um? Wird der Wert „gegenseitige Wertschätzung“ aus dem unternehmerischen Wertekanon entfernt? Sicher nicht. Gefragt ist hier vielmehr eine schnelle, unternehmensweite und eindeutige Thematisierung des Umgangs mit diesem Wert.

Eine stark oder schwach ausgeprägte Sicherheitskultur kann auch mit dem Betätigungsfeld des Unternehmens selbst verbunden sein. 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 in der Konsequenz aber nicht, dass sich im letztgenannten Umfeld Sicherheitsmaßnahmen von Haus aus wesentlich leichter implementieren lassen. Die entscheidende Frage ist auch hier: Inwieweit passen die Awareness-Aktivitäten und der damit möglicherweise einher gehende Veränderungsbedarf in den gegebenen Rahmen der Unternehmenskultur?

Corporate Identity – der Katalysator für nachhaltige Security Awareness

Security Awarenness-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 sicherheitskonformens Verhalten von vornherein auszuklammern, sondern letzten Endes auch, Ressourcen zu vergeuden. Warum? Die Corporate Identity bildet die strategische Klammer, die gleichermaßen nach innen wie auch nach aussen wirkt mit dem Ziel, einen optimalen Gesamteffekt für das Unternehmen zu erreichen (Meffert 1998). Sie bestimmt das Verhalten der Organisationsmitglieder (Corporate Behaviour), die Art und Weise, 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 (Mitarbeiterloyalität) an das Unternehmen haben. Loyale Mitarbeiter schützen das Unternehmen jederzeit, auch ohne externe Anreize – das reduziert den Umfang von „Marketingmaßnahmen“ im Kontext von Awareness-Aktivitäten deutlich, im Idealfall auf null. Zudem ist die Bereitschaft, sich Wissen anzueigenen, mit dem das Unternehmen aktiv geschützt werden kann, eine ganz andere als bei Mitarbeitern mit geringer oder gar fehlender emotionaler Bindung



2007 - 2012, HECOM Security Awareness Consulting. Alle Rechte vorbehalten. Veröffentlichung oder Kopie nur mit schriftlicher Zustimmung des Autors.

Abbildung 4. *Elemente der Corporate Identity und ihre Wirkungen*

10 Erfolgsfaktoren für nachhaltige Security Awareness

1. Bevor es losgeht: Solide Absprungbasis definieren d.h. Wo stehe ich in Sachen Security Awareness und wo will ich hin? Inwieweit ist das Ziel mit den mir zur Verfügung stehenden Ressourcen erreichbar?
2. Berücksichtigen Sie bei Planung und Durchführung Ihrer Awareness-Maßnahmen die wesentlichen Elemente Ihrer Unternehmens- und Sicherheitskultur.
3. Holen Sie sich interne Unterstützer für Ihr Vorhaben ins Boot (vor allem die Unternehmensleitung sowie wichtige „Meinungsmacher")
4. Falls erforderlich und möglich, verstärken Sie Ihr Team um Experten aus den Bereichen Kommunikation, Personal, Psychologie und Change Management.
5. Der Empfänger macht die Botschaft, nicht der Sender! Prüfen Sie den Inhalt Ihrer Policies auf Anwendbarkeit im betrieblichen Tagesgeschäft, inhaltliche Redundanz und Verständlichkeit.
6. Nicht jeder braucht alles: Identifizieren Sie die wirklich wichtigen Zielgruppen inkl. zielgruppengerechter Medien und Inhalte, die sie zum Mitmachen aktivieren.
7. Geben Sie Security ein gemeinsames Dach und etablieren sie Sicherheit als positiv besetzte „Marke" im Unternehmen.
8. Der Fächer von Awareness-Maßnahmen ist riesig. Keine Angst vor Neuem und Innovativem.
9. „Was haben wir erreicht?" Lassen Sie Ihre Awareness-Maßnahmen evaluieren. Dokumentieren Sie den Prozess und den erzielten Erfolg.
10. Security Awareness lebt von Glaubwürdigkeit und Konsequenz. Für alle Beteiligten und insbesondere für die Führungskräfte gilt: Nicht nur den anderen predigen sondern selbst tun!

an das Unternehmen. Sie werden nur das Allernötigste für das Unternehmen tun oder sich gar destruktiv gegenüber dem Unternehmen verhalten – ein Fakt der sowohl aus Sicherheitssicht als auch aus der unternehmerischen Gesamtschau kaum erstrebenswert erscheint.

Fazit:

Security Awareness-Maßnahmen implementieren will, muss sicherheitsrelevantes Wissen adäquat vermitteln und die Mitarbeiter via „Securitymarketing" dazu bringen, den Inhalt der Policies umsetzen zu wollen. Bildlich gesprochen ist man damit lediglich bei der Pflicht d.h. der Umsetzungsabsicht, die Kür in Form der tatsächlichen Umsetzung sicherheitsrelevanter Verhaltensvorgaben erfolgt eben nicht unmittelbar oder automatisch. Wirklich erfolgreich und nachhaltig wirken Security Awareness-Maßnahmen erst, wenn der Aspekt „Organisation" systematisch in die Planung und Umsetzung von Awareness-Maßnahmen miteinbezogen wird. Mit Einbezug dieses Aspekts können organisationsbedingte Stoplersteine, die die Verhaltensumsetzung be- oder verhindern identifiziert und aus dem Weg geräumt werden. Eine „gesunde" Organisation wirkt aus der Persepektive des einzelnen Organisationsmitgliedes 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 Gesamtsystem Unternehmen tagtäglich passiert, massiv beeinflusst und wirkt gleichzeitig darauf ein. Sowohl Awareness als auch Sicherheit sind somit nicht etwas „Abgekapseltes", sondern ein lebendiger Teil des Gesamtsystems Unternehmen. Will man also nicht nur Symptome kurieren, sondern vielmehr die Ursachen sicherheitsinkonformen Verhaltens aufdecken und wirksam bekämpfen, sollte möglichst umfassend und aus verschiedenen Blickwinkeln hinter die Kulissen menschlichen Handelns im Unternehmen geschaut werden (Helisch & Pokoyski 2009). Das bedeutet auch, dass bei Awareness-Aktivitäten Fragen z.B. zu Mitarbeiterloyalität und -zufriedenheit, gelebter Führung, Vertrauen und Verantwortung, Kommunikation, Konflikt- und Problemmanagement etc. 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.

Literaturhinweise:

- Frese, E. (2000) Grundlagen der Organisation. Konzept - Prinzipien – Strukturen. Wiesbaden, Gabler
- Helisch, M. & Pokoyski, D. (2009) Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden, Vieweg + Teubner
- Helisch, M. (2009 und 2011) Security Awareness in der betrieblichen Praxis. München
- Meffert, H. (1998) Marketing, Grundlagen marktorientierter Unternehmensführung, Konzepte – Instrumente – Praxisbeispiele. Wiesbaden, Gabler
- Schein, E. H. (1985) Organizational Culture and Leadership. Hoboken, Jossey-Bass
- Schreyögg, G. & Koch, J. (2007) Grundlagen des Managements. Basiswissen für Studium und Praxis. Wiesbaden, Gabler

MICHAEL HELISCH

Der Autor befasst sich seit 2002 mit dem Thema Security Awareness, hat in dieser Zeit verschiedene internationale Awareness Kampagnen konzipiert und war für deren Umsetzung verantwortlich. Michael Helisch ist Initiator der Studienreihe „Security Awareness in der betrieblichen Praxis", Referent und Autor zahlreicher Fachbeiträge und hat 2009 zusammen mit Dietmar Pokoyski das erste deutsche Praxishandbuch zum Thema Security Awareness herausgegeben.

Kontakt:

helisch@hecom-consulting.de