

# Vermitteln statt verbieten

Interview Dr. Johannes Wiele, Defense AG

Elmar Török, bits+bites

**Dr. Johannes Wiele studierte Politikwissenschaft, Philosophie und Germanistik an der Universität Münster. Nach Stationen als Fachredakteur bei Network World und LANline arbeitet er als Director Business Consulting bei der Defense AG. Dr. Wiele ist Chairman der EICAR-Taskforce „Information Security Awareness“, Mitglied der ENISA Information Awareness Community, unterrichtet an der Universität München „Psychologie der Informationssicherheit“ und ist Lehrbeauftragter der Karlsruhochschule Karlsruhe.**

**Wir sprachen mit Dr. Wiele über IT-Security Awareness im Unternehmen.**

*IT-Grundschutz: Herr Wiele, Sie sind seit langem ein dezidierter Befürworter von Awareness-Maßnahmen in Unternehmen. Was ist Ihrer Ansicht nach das größte Problem in diesem Umfeld?*

Wiele: Die wichtigste Voraussetzung ist, dass man das Problem und die Herausforderung, die in den menschlichen Komponenten der IT-Sicherheit steckt, überhaupt erkennt. Das klassische Beispiel stammt aus der Frühzeit des Internet. Kunden, die die Webseite ihrer Bank besuchten, sahen ein Fenster, in dem eine sichere Verbindung angekündigt wurde. Auswertungen der Logs des Webservers ergaben, dass ab diesem Zeitpunkt viele Benutzer aus Angst etwas falsch zu machen den Vorgang abbrachen. Der Begriff „sichere Verbindung“ irritierte die Leute mehr, als dass es sie beruhigte.

*IT-Grundschutz: Wäre da gestanden „Ab jetzt ist es sicher“, hätte es weniger Schwierigkeiten gegeben.*

Wiele: Ja, das stand da aber nicht. Der Programmierer, der die SSL-Verbindung vorgesehen hat, sah das Problem „unsichere Verbindung“ als gelöst an. Aber für normale Anwender war das zu verklausuliert und ominös – die wussten einfach nicht, was sie davon halten sollen. Man hätte mehr Informationen mitliefern sollen, was eigentlich sicher wird und gegen was die Sicherung

schützt. Und mittlerweile wurde ja tatsächlich reagiert – es gibt dieses kleine Schlosssymbol bei SSL und einige Änderungen am Benutzerinterface. Aber es hat lange gedauert, bis das Thema verstanden und gelöst war.

*IT-Grundschutz: Und solche Dinge passieren jetzt nicht mehr?*

Wiele: Doch, aber in anderer Form. Es gibt in der Industrie immer eine Tendenz, Sicherheitsmaßnahmen einzuführen, ohne wirklich an die Folgen zu denken. Die Folgen können positiv, aber auch negativ sein. Eine Verbesserung der Sicherheitslage erreicht man nur, wenn die Mitarbeiter verstehen, was man da tut und warum. Man muss Akzeptanz erreichen, und das ist nicht einfach. Dazu ist eine Menge Erklärungsaufwand nötig, man muss die Leute wirklich erreichen und so guten Kontakt zu ihnen pflegen, dass man auch mitbekommt, ob man sie mit den Sicherheitsmaßnahmen überhaupt erreicht.

*IT-Grundschutz: Und Sie glauben, dass Firmen zu schnell mit einschränkenden Maßnahmen zu Hand ist?*

Wiele: Zu schnell und manchmal zu leichtfertig. Sie vernachlässigen die Nebenwirkungen. Sehen Sie sich als Beispiel eine Forsa-Studie vom Januar 2010 an. Darin sagen 67 Prozent der Deutschen, dass der Einsatz von Körperscannern an Flughäfen für

mehr Sicherheit beim Fliegen sorgt. Die Industrie schlussfolgert, dass Körperscanner an Flughäfen damit eine breite Mehrheit haben. Aber die Studie gibt keine Auskunft darüber, ob die Befragten für die zusätzliche Sicherheit auch die Nachteile in Kauf nehmen, ob sie den Einsatz der Scanner also akzeptieren oder ob sie zum Beispiel weniger oft fliegen werden. Hier liegt meiner Ansicht nach das Problem: Industrie und Gesetzgeber tun zu wenig, um einschränkende Verfahren akzeptabel zu machen.

*IT-Grundschutz: Wer Sicherheit durchsetzen will, muss immer die Komfortzone von Menschen beschneiden. Akzeptanzprobleme sind da vorprogrammiert.*

Wiele: Stimmt, aber es kommt eben darauf an, wie man die Beschränkungen umsetzt. Zurzeit liegt es etwa stark im Trend, die USB-Ports zu sperren oder nur die Nutzung von ganz bestimmten USB-Sticks zu erlauben. Das ist legitim und hat natürlich auch gute Gründe. Doch wenn Sie mit so einer Maßnahme verhindern, dass ein Mitarbeiter Aufgaben erfüllen kann, die er laut seiner Tätigkeitsbeschreibung durchführen muss, laden Sie geradezu zu aktivem und passivem Widerstand ein. Dann nimmt auch die Person oder, noch schlimmer, die Abteilung Schaden, die diese Regel erdacht und eingeführt hat.

*IT-Grundschutz: Und wie kommt man an diesem Problem vorbei?*

Wiele: Man muss die Auswirkungen der Maßnahme aus Sicht des Mitarbeiters sehen und ihm zeigen, dass man ihn ernst nimmt. Ein beliebtes Beispiel sind WLAN-Verbindungen an öffentlichen Orten. Es mag ja sein, dass diese aus Sicherheitsgründen nicht erlaubt sind. Aber wenn der Mitarbeiter von unterwegs eine Präsentation oder Daten schicken muss, kommt es automatisch zum Konflikt. Dafür gibt es zwei Abhilfen: Entweder, man zieht die Priorität der Sicherheitsmaßnahme durch und sagt: „Sicherheit ist wichtiger als Präsentation, dann schickst Du die eben nicht, das ist in Ordnung.“ Oder man bietet für solche Fälle einen Work-Around an, der das Senden ausnahmsweise erlaubt.

*IT-Grundschutz: Mehraufwand oder Frust für den Mitarbeiter ist das trotzdem.*

Wiele: Mehraufwand vielleicht, aber Frust nicht. Benutzer akzeptieren einschränkende Regeln, wenn sie wissen, dass diese sinnvoll sind. Wer als Betroffener in der gerade beschriebenen Situation das Feedback bekommt: „Die Sicherheit ist wichtiger, lass die Präsentation“, der kann auch mit solch einer Regel leben, weil er weiß, dass seine Position ernst genommen wird.

*IT-Grundschutz: Das hat aber weniger mit IT-Sicherheit zu tun, als mit dem generellen Verständnis für die Prozesse und Prioritäten im Unternehmen.*

Wiele: Exakt, das ist der entscheidende Punkt bei allen Sicherheitsmaßnahmen. Es ist wichtig, die Notwendigkeiten für die Anwender zu verstehen. Nur so gewinnt man die aktive Hilfe der Benutzer. Ohne dieses Vorgehen gibt es keinen Sicherheitsgewinn. Sicherheit ist ja in allen Bereichen wichtig – bei einem Telefonat am Flughafen, beim Arbeiten im Zug: Das kriegt man nur hin, wenn jeder selbst für Sicherheit eintritt. Signalisiert man



Dr. Johannes Wiele, Director Business Consulting, Defense AG

der Belegschaft: „Ihr seid nur ein Risiko“, verletzt man deren Selbstwertgefühl und verliert deren Loyalität.

*IT-Grundschutz: Das ist leicht gesagt, aber wie bekommt man die Ansprache richtig hin?*

Wiele: Über so etwas kann man nur reden, wenn man sich die Situation im Unternehmen genau angesehen hat. Sicherheitsmaßnahmen werden in jeder Umgebung anders gesehen. An einer Produktionsstraße würde kein Mitarbeiter auf die Idee kommen, auf dem Steuerungs-PC für einen Stanzautomaten eigene Software zu installieren. Da kann man die USB-Ports und andere Zugangswege problemlos abriegeln. Im kreativen Umfeld, wo es die Leute gewöhnt sind, fast alles mit ihren Rechnern anstellen zu dürfen, und davon auch für ihre Arbeit profitieren, ist das ganz anders. Das Regelwerk muss sich mit dem Selbstverständnis der Angestellten und ihrer Sichtweise der eigenen Aufgabe und Position decken.

*IT-Grundschutz: Wenn man die zahlreichen Awareness-Anbieter ansieht, scheint es viel Nachholbedarf in dieser Hinsicht zu geben.*

Wiele: Wer gibt denn heute normalerweise Sicherheitsregeln vor? Das sind CIOs und CSOs, denen IT-Sicherheit ausschließlich über die

Technik vermittelt wurde. Ihnen fehlt meistens der Blick für die sozialen Aspekte. Man kann ihnen das auch nicht vorwerfen, sie haben es einfach nicht gelernt. Heute müssen Studenten technischer Fächer oft auch zu psychologischen oder sozialpädagogischen Seminaren. Das ist zumindest ein Ansatz. In einigen Jahren wird man sehen, ob er fruchtet.

*IT-Grundschutz: Mit welchen negativen Reaktionen muss man rechnen, wenn Sicherheitsmaßnahmen „durchgedrückt“ werden?*

Wiele: Als erstes schränken die Mitarbeiter ihre Leistung für das Unternehmen ein. Das ist eine typische Trotzreaktion auf Einschränkungen, die so genannte „Reaktanz“: „Wenn Ihr mir das Leben schwer macht, dann mache ich nur noch Dienst nach Vorschrift“. Zweitens kann man oft das Abwälzen von Verantwortung beobachten. Das Motto heißt dann: „Wenn ihr mich nicht einbezieht, geht mich das auch nichts an, macht Euren Sicherheitskram doch alleine.“ Und drittens gibt es immer technisch versierte Mitarbeiter, die einen Weg um die Maßnahmen herum suchen und meist auch finden. Unsensible und schlecht formulierte Sicherheitsmaßnahmen haben den gegenteiligen Effekt, zumindest bei den Kosten.

*IT-Grundschutz: Herr Wiele, ganz konkret, wie vermeide ich eine solche Situation?*

Wiele: IT-Sicherheit darf nicht allein vom technischen Standpunkt aus geplant werden. Holen Sie jemanden dazu, der sich die Businessprozesse mit den Mitarbeitern anschaut. Welche Auswirkungen hat meine Maßnahme organisatorisch? Mache ich etwas kaputt, was die Mitarbeiter im Arbeitsalltag benötigen? Eigentlich sollten Sie auch eine zumindest rudimentäre Erfassung des Wissen und Könnens der Mitarbeiter durchführen: Was

kann ich ihnen zumuten, womit können sie umgehen? Und ganz wichtig: Lassen Sie Rückkopplung zu. Wenn keine gesetzlichen Vorgaben dagegen sprechen, können Sie die Maßnahmen doch mit den Mitarbeitern oder zumindest den Fachbereichsleitern gemeinsam entwickeln. Geben Sie den Leuten in irgendeiner Form Gelegenheit, sich daran zu beteiligen. Das ist an sich schon die perfekte Awareness-Schulung, und sie funktioniert auch in kleineren Firmen recht gut.

*IT-Grundschutz: Und was tue ich, wenn das Kind schon im Brunnen liegt und ein Sicherheitsprojekt am Widerstand und Desinteresse scheitert?*

Wiele: Man muss die Situation dann wirklich offen ansprechen, um irgendwie wenigstens zum Zustand von vorher zurückzukommen. Sagen Sie: „Wir haben es verstanden, das läuft falsch, wir machen es jetzt noch Mal von vorn und dieses Mal mit eurem Input“. Das sind ganz einfache Dinge, aber die müssen getan werden.

*IT-Grundschutz: Das sagen Sie so einfach, aber da steckt ja unter Umständen schon viel Geld drin – und wie erreiche ich die Leute überhaupt?*

Wiele: In größeren Firmen gibt es oft so etwas wie einen internen Fernsehkanal, mit dem lassen sich solche Botschaften gut vermitteln. Oder veranstalten Sie Kick-Off Meetings, für die ganze Firma oder für die Abteilungen. Es kommt aber ganz auf die Firma an, beim kleinen Familienunternehmen etwa ist „ein Wort des Patriarchen“ oft viel wirkungsvoller als alles andere. Wichtig ist immer, die echten Vertrauenspersonen im Betrieb zu finden und diejenigen, die die Meinungsführerschaft inne haben. Das sind die Leute, die man gewinnen muss.

*IT-Grundschutz: Und wie kann ich den Betriebsrat einbinden?*

Wiele: Formal führt daran ohnehin kein Weg vorbei, denn viele Sicherheitsmaßnahmen lassen sich nun mal tatsächlich als Leistungsmessung der Mitarbeiter missbrauchen. Binden Sie den Betriebsrat also so früh wie möglich ein. Stellen Sie klar, dass die Sicherheitsmaßnahmen für die Mitarbeiter auch eine Fortbildung darstellen. Man muss unbedingt ehrlich sein und seine Ziele klar formulieren. Ideal ist es, wenn bei großen Projekten ein neutraler Partner beteiligt ist, beispielsweise eine Universität.

*IT-Grundschutz: Wägen Sie eine Prognose: Wie wird sich Awareness in Zukunft verändern?*

Wiele: Es wird immer mehr zum festen Bestandteil der IT-Sicherheit werden. In den USA finden Sie schon seit langem Ausschreibungen für die Position des CSO, in denen soziale Kompetenzen und eine psychologische Grundausbildung gefordert werden. In Deutschland kommt dies gerade erst auf. Obwohl also die USA eher den Ruf des rustikalen Umgangs mit Mitarbeitern haben, wird dort die zielgruppengerechte Vermittlung des Sicherheitswissens eher als notwendige Aufgabe erkannt. Dies ist auch eine Ansage an die ausbildenden Institutionen. Sie müssen psychologische Faktoren stärker einbeziehen. An der Ludwig-Maximilians-Universität in München tun wir das bereits. Generell macht der Bachelor/Master im Moment Schwierigkeiten, denn er erschwert es, selbstbestimmt fachübergreifend zu studieren. Aber auch das wird sich nach einer Weile einspielen, wenn sich die Studienpläne entsprechend anpassen.

*IT-Grundschutz: Herr Wiele, wir danken Ihnen für dieses Gespräch.*

## Hier abonnieren



## IT-Grundschutz

### Diese Leser profitieren vom Informationsdienst IT-Grundschutz

- IT-Leiter
- Administratoren
- Sicherheitsbeauftragte
- Bezieher der IT-Grundschutzkataloge
- Datenschutzbeauftragte
- IT-Security-Officer zum schnellen Überblick und zur Weitergabe an Geschäftsleitung, IT-Leitung oder Administratoren.
- Für die Sicherheits-Verantwortlichen in Behörden und mittelständischen Unternehmen, in denen es keinen speziellen IT-Security-Officer gibt

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

### Abonnement-Bestellung an Fax +49 6725 5994

**Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschutz“ ab Ausgabe \_\_\_\_\_ zum Jahresbezugspreis (10 Ausgaben, davon 2 Doppelausgaben) von 98,00 € (Inland) / 116,10 € (Ausland) inkl. MwSt. und Versandkosten (Schweiz: 187,00 SFr).**

Ich kann das Abonnement jederzeit kündigen. Zuviel bezahlte Abo-Gebühren werden rückerstattet. Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weiterleiten kann.

Absender / Firmenstempel \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Datum

Zeichen

Unterschrift

Die SecuMedia Verlags GmbH räumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen.

## SecuMedia

Der Verlag für  
Sicherheits-Informationen

SecuMedia Verlag  
Postfach 12 34, 55205 Ingelheim  
vertrieb@secumedia.de  
Tel. +49 6725 9304-0