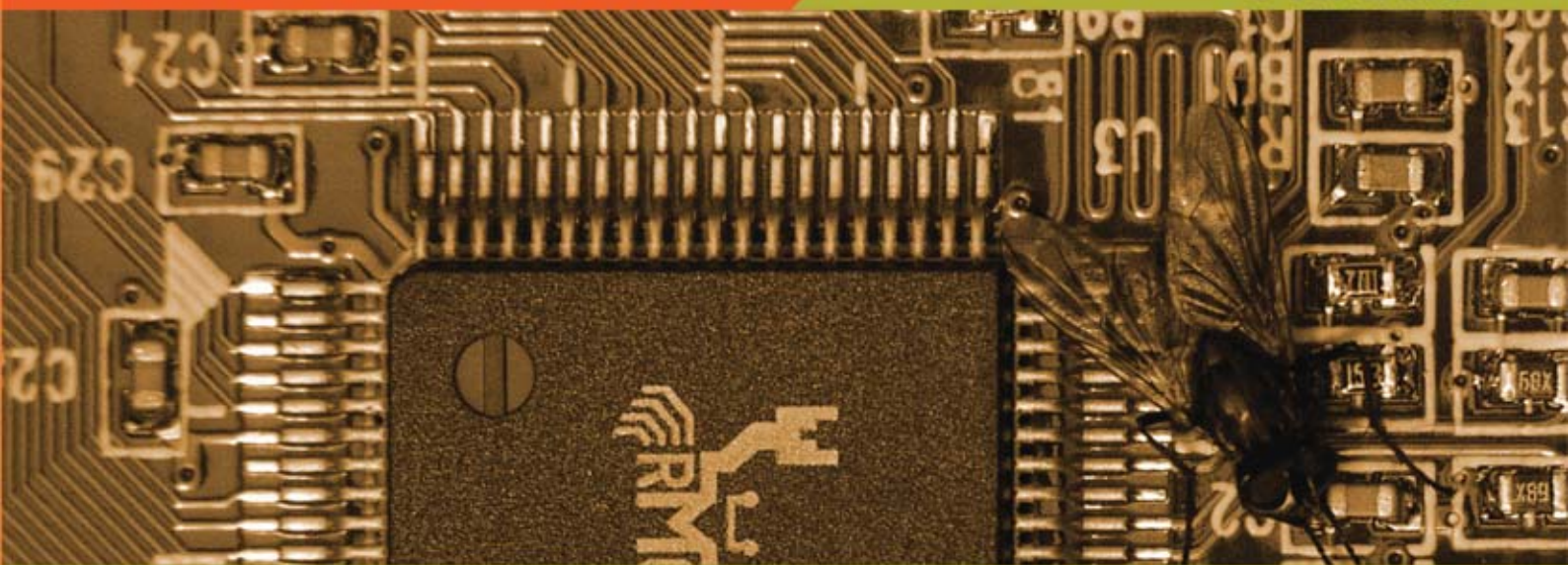


Sebastian Klipper

# Konfliktmanagement für Sicherheitsprofis

Auswege aus der „Buhmann-Falle“ für  
IT-Sicherheitsbeauftragte, Datenschützer und Co

**PRAXIS**



  
VIEWEG+  
TEUBNER

<kes>

Sebastian Klipper

Konfliktmanagement für Sicherheitsprofis

Sebastian Klipper

# Konfliktmanagement für Sicherheitsprofis

Auswege aus der „Buhmann-Falle“ für  
IT-Sicherheitsbeauftragte, Datenschützer und Co

Mit 63 Abbildungen und 25 Tabellen

PRAXIS



**VIEWEG+  
TEUBNER**

Bibliografische Information der Deutschen Nationalbibliothek  
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der  
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über  
<<http://dnb.d-nb.de>> abrufbar.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2010

Alle Rechte vorbehalten

© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2010

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.

Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.

[www.viewegteubner.de](http://www.viewegteubner.de)



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg

Umschlagbild: Sebastian Klipper

Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Printed in Germany

ISBN 978-3-8348-1010-6

Für Eva.

## **Dank**

Dank gilt meinem Deutschlehrer Dr. Volkmar Stein. Für sein Engagement um den Literarischen Salon in meiner Heimatstadt Büdingen wurde er mit dem Verdienstorden der Bundesrepublik Deutschland ausgezeichnet. Tut mir leid, mein erstes Buch ist leider kein Roman geworden.

Dank gilt auch den zwei Dienststellenleitern Oberst a.D. Nitschke und Generalmajor Fürst, die mir in Sachen Sicherheit stets den Rücken gestärkt haben – ein Glücksfall, den man nicht immer haben kann.

Außerdem möchte ich all meinen Mitstreitern danken, mit denen ich in den vielen Jahren als IT-Sicherheitsbeauftragter intensiv an neuen Ideen und Sicherheitslösungen arbeiten konnte.

# Vorwort

Sachbücher sollen anlockend sein. Das werden sie nur, wenn sie die heiterste und zugänglichste Seite des Wissens darbieten. Das wusste schon Goethe. Und Voltaire setzt dem hinzu, dass das Geheimnis zu langweilen darin bestünde, alles zu sagen. Der Ratschlag an den Autor eines Sachbuchs lautet nach diesen beiden Regeln: *„Auf heitere und zugängliche Art einige Dinge weglassen, die sich der Leser bitte selbst erschließen möge.“*

Dieses Buch möchte mit den nötigen Mitteln wappnen, die den Weg durch die Untiefen der Security-Kommunikation weisen. Dabei soll es nicht so verstanden werden, dass technische Sicherheitsmaßnahmen nicht erfolgreich sein könnten. Sie sind und bleiben weiter wichtig. Das wäre der Teil, den sich der Leser dazu denken müsste, ohne dass es immer wieder gesagt wird. Dieses Buch versucht vielmehr, den Fokus des Lesers in eine Richtung zu lenken, die bisher zu sehr vernachlässigt wurde.

Während sich schon seit Lange Bücher<sup>1</sup> damit befassen, wie man den Mensch dazu bringt, gegen Sicherheitsregeln zu verstoßen, gibt es nur wenige Bücher<sup>2</sup>, die sich das Gegenteil zum Schwerpunkt machen. Dabei sind sich die meisten Experten einig, dass der Mensch der Risikofaktor Nummer Eins ist. Es gibt hunderte Bücher über Firewalls, Betriebssystem-Sicherheit, Security-Scanner oder die richtige Konfiguration eines Apache-Webserver. Es gibt aber kaum welche darüber, wie man Entscheider dazu bringt, die nötigen Mittel für Sicherheitsmaßnahmen zur Verfügung zu stellen oder wie man die Mitarbeiter motiviert, keine Wettbewerbe im Umgehen von Sicherheitsmaßnahmen zu veranstalten.

Am Ende des Buchs wird einer der 10 Leitsätze zum Konfliktmanagement lauten: *„Im Mittelpunkt jeder Sicherheitsbetrachtung steht menschliches Handeln und Unterlassen.“* In diesem Sinne wünsche ich Ihnen viel Spaß bei der Lektüre und viele neue Ideen, wie Sie die Sicherheit in Ihrem Unternehmen oder Ihrer Behörde voran bringen können.

---

<sup>1</sup> Kevin Mitnick; Die Kunst der Täuschung; 2003; mitp; ISBN 3-8266-1569-7

<sup>2</sup> Pokoyski, Dietmar / Helisch, Michael (Hrsg.); Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung; 2009; ISBN: 978-3-8348-0668-0

# Inhaltsverzeichnis

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Dank .....                                                        | V   |
| Vorwort .....                                                     | VII |
| Inhaltsverzeichnis .....                                          | IX  |
| Einführung .....                                                  | 1   |
| 1 Willkommen auf der Security-Bühne .....                         | 5   |
| 1.1 Geschäftsleitung, Behördenleitung und oberes Management ..... | 8   |
| 1.2 Sicherheitsexperten .....                                     | 13  |
| 1.2.1 Sicherheitsbeauftragte .....                                | 15  |
| 1.2.2 Datenschutzbeauftragte .....                                | 18  |
| 1.2.3 IT-Sicherheitsbeauftragte .....                             | 21  |
| 1.2.4 Die drei Musketiere .....                                   | 25  |
| 1.2.4.1 Fallbeispiel: Das Pharma-Unternehmen ExAmple AG .....     | 26  |
| 1.3 Mitarbeiter .....                                             | 28  |
| 1.3.1 Fallbeispiel: Das Angebots-Fax .....                        | 30  |
| 1.4 Personal- und Interessenvertretungen .....                    | 36  |
| 1.5 Zusammenfassung .....                                         | 37  |
| 2 Arten von Security-Konflikten .....                             | 39  |
| 2.1 Was sind Security-Konflikte .....                             | 40  |
| 2.2 Verhaltenskreuz nach Schulz von Thun .....                    | 43  |
| 2.2.1 Fallbeispiel: Das Angebots-Fax .....                        | 45  |
| 2.3 Normenkreuz nach Gouthier .....                               | 46  |
| 2.4 Interessenkonflikte .....                                     | 50  |
| 2.4.1 Die „Zweit-Job-Falle“ .....                                 | 51  |
| 2.4.2 Wer kontrolliert den Kontrolleur? .....                     | 53  |
| 2.5 Vertrauensverlust durch Sicherheitsmaßnahmen .....            | 54  |

|         |                                                                                 |     |
|---------|---------------------------------------------------------------------------------|-----|
| 2.6     | Fallbeispiel: Mehr Unterstützung vom Chef .....                                 | 57  |
| 2.7     | Zusammenfassung .....                                                           | 59  |
| 3       | Konfliktprävention .....                                                        | 61  |
| 3.1     | Konfliktpräventive Kommunikation.....                                           | 62  |
| 3.2     | Gemeinsames Vokabular .....                                                     | 67  |
| 3.2.1   | Informationssysteme .....                                                       | 68  |
| 3.2.2   | Sicherheit .....                                                                | 71  |
| 3.2.2.1 | In English please: certainty, safety, security,<br>protection, privacy etc..... | 72  |
| 3.2.2.2 | Gegenüberstellung: Datenschutz vs. Informationssicherheit.....                  | 74  |
| 3.2.3   | Die Sicherheitspräfixe IT, IV, IS und I .....                                   | 76  |
| 3.2.4   | Corporate Security .....                                                        | 79  |
| 3.3     | Konfliktpipeline.....                                                           | 81  |
| 3.3.1   | Fallbeispiel: Unbegleitete Besuchergruppen.....                                 | 86  |
| 3.4     | Motivation.....                                                                 | 88  |
| 3.4.1   | Was ist Motivation.....                                                         | 89  |
| 3.4.2   | Motivation von Geschäfts- und Behördenleitung.....                              | 92  |
| 3.4.2.1 | Live-Vorfürungen/ Live-Hacking .....                                            | 94  |
| 3.4.2.2 | Penetrations-Tests .....                                                        | 98  |
| 3.4.2.3 | Fallbeispiel: Live-Vorführung und Pen-Test<br>in der ExAmple AG.....            | 102 |
| 3.4.3   | Motivation der Mitarbeiter.....                                                 | 103 |
| 3.4.3.1 | Awareness-Kampagnen.....                                                        | 106 |
| 3.4.3.2 | Kleine Schupse.....                                                             | 109 |
| 3.4.3.3 | „drive-by“-Risikoanalysen .....                                                 | 114 |
| 3.4.4   | Eigenmotivation und der Umgang mit Frustration.....                             | 118 |
| 3.5     | Zusammenfassung .....                                                           | 122 |
| 4       | Sicherheits-„Hebel“ .....                                                       | 125 |
| 4.1     | Security by .....                                                               | 126 |
| 4.1.1   | Security by tradition .....                                                     | 126 |

---

|         |                                                         |     |
|---------|---------------------------------------------------------|-----|
| 4.1.2   | Security by concept.....                                | 128 |
| 4.2     | Good Cop – Bad Cop.....                                 | 130 |
| 4.2.1   | Positive Nachrichten generieren.....                    | 131 |
| 4.2.1.1 | Fallbeispiel: Alles bestens in der ExAmple AG.....      | 133 |
| 4.2.2   | Negative Nachrichten meistern .....                     | 135 |
| 4.2.2.1 | Fallbeispiel: Alles schrecklich in der ExAmple AG ..... | 138 |
| 4.3     | Security-Storyboard.....                                | 141 |
| 4.3.1   | Erster Akt: Panik.....                                  | 141 |
| 4.3.2   | Zweiter Akt: Rückfall .....                             | 143 |
| 4.4     | Security braucht Avatare .....                          | 145 |
| 4.4.1   | Fallbeispiel: Herkules und der Stall des Augias .....   | 148 |
| 4.5     | Security ist Cool.....                                  | 152 |
| 4.6     | Tue Gutes und rede darüber.....                         | 155 |
| 4.7     | Zusammenfassung .....                                   | 157 |
| 5       | Krisenbewältigung .....                                 | 159 |
| 5.1     | Der Umgang mit Widerstand .....                         | 160 |
| 5.1.1   | Fallbeispiel: Bob platzt der Kragen.....                | 162 |
| 5.2     | Eskalationsstufen generieren.....                       | 164 |
| 5.2.1   | Fallbeispiel: Die ExAmple AG „eskaliert“ .....          | 168 |
| 5.3     | Diskretion bei Sicherheitsvorfällen .....               | 170 |
| 5.4     | Krisen-PR.....                                          | 174 |
| 5.5     | Wenn die Unterstützung von höchster Stelle fehlt .....  | 179 |
| 5.6     | Zusammenfassung .....                                   | 182 |
| 6       | Am Ende kommt der Applaus .....                         | 183 |
| 6.1     | Leitsätze zum Konfliktmanagement .....                  | 184 |
| 6.1.1   | Satz 1 – Problemfelder.....                             | 184 |
| 6.1.2   | Satz 2 – Nur im Team .....                              | 184 |
| 6.1.3   | Satz 3 – Kommunikation ist Alles.....                   | 184 |
| 6.1.4   | Satz 4 – Der Mensch.....                                | 185 |
| 6.1.5   | Satz 5 – Die Technik.....                               | 185 |

|                          |                                      |     |
|--------------------------|--------------------------------------|-----|
| 6.1.6                    | Satz 6 – Gemeinsames Vokabular ..... | 185 |
| 6.1.7                    | Satz 7 – Marketing .....             | 185 |
| 6.1.8                    | Satz 8 – Motivation .....            | 186 |
| 6.1.9                    | Satz 9 – Neue Ideen.....             | 186 |
| 6.1.10                   | Satz 10 – Erfolg.....                | 186 |
| Sachwortverzeichnis..... |                                      | 187 |

# Einführung

Wenn Sie dieses Buch zum ersten Mal in den Händen halten und vor der Wahl stehen, ob Sie es kaufen sollen oder nicht, dann empfehle ich Ihnen direkt zum Kapitel *Willkommen auf der Security-Bühne* auf Seite 5 zu springen. Dort wird eine Szenerie beschrieben, wie sie Datenschützer, IT-Sicherheitsbeauftragte und Co. jeden Tag erleben können. Für diese und andere Problemsituationen liefert dieses Buch Lösungsmöglichkeiten.

Was macht die Probleme der Sicherheitsprofis so speziell? Wenn es keine Sicherheitsvorfälle gibt, will niemand all die Datenschutzbeauftragten, Sicherheitsbeauftragten oder Information Security Officers sehen. Sie gelten als Spielverderber, Bedenkenträger und Fortschrittsverhinderer. Viele Sicherheitsexperten stoßen auf Schwierigkeiten, wenn sie ihre Botschaft unter die Leute bringen wollen, was umso unverständlicher ist, weil sie meist genau dafür bezahlt werden. Ist das Kind erst in den Brunnen gefallen, wird der oder die Schuldige gesucht. *„Warum haben die Security-Leute nichts dagegen unternommen?“* Die Security-Welt ist voller Missverständnisse und Konflikte, die ein hohes Maß an Kommunikationsstärke und Konfliktfähigkeit erfordern. Dabei kann ein Job in der Security-Branche durchaus Spaß machen, wenn man sich auf die beteiligten Akteure, ihre Sorgen und Zwänge besser einstellt.

Welcher Sicherheitsprofi kennt das nicht: Sicherheitsmaßnahmen lösen Widerstand aus und sorgen für Konflikte? Sicherheitsprofis leben tagein, tagaus mit Begriffen wie *Bedrohung*, *Risiko* oder *Schwachstelle*. Die Security-Branche ist eine Mausefalle. Wer einmal in dieser Falle gefangen sitzt, findet selten den Ausgang, der zurück in den vormaligen Geisteszustand leitet.<sup>3</sup> In den meisten Fällen stand die Tätigkeit nicht einmal auf dem Berufswunschzettel.<sup>4</sup> Mit der Zeit geht das Wissen darüber verloren, wie viel oder wie wenig der mitbringt, der das Büro der Sicherheitsprofis zum ersten Mal betritt.

Stöbert man in der Buchhandlung durch das Angebot an Konfliktliteratur, wird man mit einem fast unüberschaubaren Angebot konfrontiert. Eine Vielzahl von Büchern versprechen Lösungen für die Konflikte des Alltags. Betrachtet man als IT-Sicherheitsbeauftragter, Datenschützer oder Sicherheitsbeauftragter dann die

---

<sup>3</sup> Frei nach Egmont Colerus, der den Vergleich für die Mathematik benutzt; Vom Einmaleins zum Integral; 1947; Zsolnay; ASIN: B0000BH6NV

<sup>4</sup> known\_sense (Herausgeber u.a.); Aus der Abwehr in den Beichtstuhl – Qualitative Wirkungsanalyse CISO & Co.; 2008; known\_sense; Seite 11

Inhaltsverzeichnisse und Buchrücken, so stellt man fest, dass sich immer nur ein sehr kleiner Teil des Inhalts auf den eigenen beruflichen Alltag anwenden lässt. Die Kernprobleme, denen sich die Sicherheitsprofis jeden Tag stellen müssen, werden meist nur am Rande betrachtet. Das vorliegende Buch fasst die wichtigsten Erkenntnisse und Erfahrungen aus Literatur und Praxis zusammen und wendet sie auf die Herausforderung Security-Job an:

Im ersten Kapitel über die Security-Bühne werden die Hauptakteure vorgestellt, mit denen die Beauftragten für Sicherheit, IT-Sicherheit und Datenschutz zu tun haben - allen voran die Chefs. Wie erreicht man es, sie auf die „*sichere Seite*“ zu locken? Welche Themen sind ihnen besonders wichtig und wie kann man sie für das Thema Sicherheit gewinnen? Nicht weniger wichtig sind die Mitarbeiter und deren Interessenvertretungen. Welche Rollen vertreten sie? Schon im ersten Kapitel werden die Knackpunkte angesprochen, die es im Verlauf des Buchs zu vertiefen gilt. Fallbeispiele aus der Praxis veranschaulichen die Themen vom ersten bis zum letzten Kapitel.

Nachdem im ersten Kapitel die Hauptakteure unter die Lupe genommen wurden, befasst sich Kapitel 2 mit der Frage, was Security-Konflikte sind und was sie von anderen Konflikten unterscheidet. Warum geraten gerade IT-Sicherheitsbeauftragte, Datenschützer und Co. immer wieder in die „*Buhmann-Falle*“ und was ist zu tun, um das in Zukunft zu vermeiden? Neben theoretischen Tools, wie dem Verhaltenskreuz und dem Normenkreuz stellen weitere Fallbeispiele den Bezug zur Praxis her. Ein besonderes Augenmerk liegt auf einer ganz besonderen Art von Konflikten, die Sicherheitsprofis selbst betreffen: Interessenkonflikte. Was tun, wenn Security nur der Zweit- oder gar Dritt-Job ist?

Besser als in Security-Konflikten festzustecken und sie als solche zu erkennen ist natürlich, sie erfolgreich zu bewältigen und sie nicht eskalieren zu lassen. Die richtige Kommunikations- und Motivationsstrategien sind Inhalt des dritten Kapitels. Wie vermeidet man durch eine klare Kommunikation konsequent die Art von Missverständnissen, die in den ersten beiden Kapiteln betrachtet wurden? Wie motiviert man mit Live-Hackings und Penetration-Tests auch den unmotiviertesten Chef und welche Bedeutung haben Awareness-Kampagnen für die Mitarbeiter-Motivation. Nicht zuletzt stellt sich die Frage, wie man sich als Sicherheitsprofi selbst motiviert – immerhin scheint man einen schier aussichtslosen Kampf gegen Sicherheitsvorfälle zu führen – 100% Sicherheit gibt es eben nicht.

Neben all diesen Möglichkeiten stellt sich die Frage, welche weiteren Blickwinkel sich anbieten, um Informationssysteme zu beleuchten. Wie kann man Stellen finden, an denen man mit weiteren Hebeln ansetzen kann, um die Sicherheitskultur des Unternehmens oder der Behörde in der man tätig ist, voran zu treiben. Das vierte Kapitel greift diese Blickwinkel und Hebel auf und möchte

Denkansätze bieten, die es ermöglichen, sich weiteres Potential in der Verbesserung der Sicherheitskultur zu erschließen. Dazu gehört für Sicherheitsprofis auch eine gesunde Portion Marketing in eigener Sache und das Selbstbewusstsein, die gemeinsam erreichten Erfolge zu kommunizieren. „*Security ist Cool*“ lautet daher eine wesentliche Botschaft des vierten Kapitels, das Sicherheitsprofis darüber hinaus dazu aufruft: „*Tue Gutes und rede darüber*“.

Was aber gibt es für Möglichkeiten, wenn der Widerstand der Mitarbeiter überhandnimmt und einfach nichts funktionieren will? In solchen Fällen ist es notwendig, den strittigen Sicherheitsmaßnahmen in geregelten Eskalationsstufen Gehör zu verschaffen. Das fünfte Kapitel beschäftigt sich aber nicht nur damit. Es beleuchtet auch den Umgang mit der internen und externen Kommunikation von Sicherheitsvorfällen. Wie bremst man die Gerüchte-Küche und wie informiert man Mitarbeiter, Chefs und Öffentlichkeit in einer Situation, in der man eigentlich mit dem Sicherheitsvorfall beschäftigt ist. Die letzte große Herausforderung ist es, wenn die Unterstützung von höchster Stelle fehlt und die Sicherheitsprofis auf scheinbar verlorenem Posten stehen.

Erst, wenn IT-Sicherheitsbeauftragte, Datenschützer und Co. all diese Klippen umschiffen haben, kommen sie allmählich wieder in ruhigeres Fahrwasser. Im sechsten Kapitel wird es Zeit Resümee zu ziehen und die Inhalte der bisherigen Kapitel komprimiert darzustellen. Das Buch schließt daher mit 10 Leitsätzen zum Konfliktmanagement, die den Inhalt des Buchs auf kurze, prägnante Formeln bringen, die in der täglichen Arbeit wichtig sind.



Die meisten von uns haben in der Schule gelernt, nichts in Bücher zu schreiben. Das halte ich für einen großen Fehler. Wahrscheinlich könnte man den Notenschnitt an deutschen Schulen deutlich heben, wenn Schüler in ihre Bücher schreiben dürften. Ich möchte Sie daher einladen, sich im Buch Notizen zu machen. Sie werden das Buch dann wahrscheinlich nicht mehr gebraucht verkaufen können, aber Sie erhöhen den Wert für sich dadurch um ein Vielfaches. Lesen Sie dieses Buch am besten immer mit einem Stift in der Hand. Streichen Sie an, was immer Ihnen gefällt, und streichen Sie durch, was für Ihre konkrete Situation uninteressant ist. Wenn die Stelle in einem Jahr für Sie wichtig wird werden Sie sie schnell wiederfinden. Streichen Sie nicht nur an und durch; kommentieren Sie und nummerieren Sie sich Denkschritte am Rand mit. So werden auch eher theoretische Abschnitte zum ganz praktischen Arbeitsabschnitt. Welchen Vorteil sollte man sonst haben ein Buch zu kaufen? Nutzen Sie diese Möglichkeiten.

Das Buch enthält zahlreiche Quellenangaben und Literaturhinweise. Soweit es möglich war, habe ich versucht meine Aussagen durch offene Quellen im Internet zu belegen. Dadurch ist es möglich, sich mit wenigen Klicks und mit Hilfe der Google Buchsuche unter <http://books.google.de> nach weiterführender Literatur umzusehen. Die Bücher auf google.de sind zwar teilweise nur als eingeschränkte Vorschau verfügbar, diese reicht aber meist aus, sich ein Bild davon zu machen, ob sich der Kauf eines Buchs lohnt oder nicht – ähnlich einem Durchblättern im Buchladen.

Bei Gesetzen und Standards können die Quellen auch leicht als PDF gefunden werden. Auf einen Link habe ich verzichtet, da sich die URLs mit der Zeit ändern. Sie werden die Dokumente in jeder leistungsfähigen Suchmaschine finden. Diese im Internet verfügbaren „*Papier-Quellen*“ sind am Ende der Fußnote durch ein solches Fähnchen gekennzeichnet: 

Online-Quellen wurden jeweils mit Angabe der URL und des Datums der Einsichtnahme aufgeführt. Einige Seiten, bei denen eine Veränderung sehr wahrscheinlich ist, wurden zusätzlich in dem Zustand, in dem sie gesichtet wurden auf <http://www.webcitation.org> archiviert. Alle Links des Buchs können über den OnlinePLUS-Service abgerufen werden.

# 1 Willkommen auf der Security-Bühne

*Die ganze Welt ist wie eine Bühne, wir stolzieren und ärgern uns ja ein Stündchen auf ihr herum, und dann ist unsere Zeit um. Doch was hat es mit der Bühne auf sich und mit den Gestalten, die sie bevölkern?*

*Erving Goffman<sup>5</sup>*

Für Erving Hoffman ist die ganze Welt wie eine Bühne. In den Mittelpunkt seines Interesses stellt er die Menschen und mit Recht fragt er, was es mit ihnen auf sich hat. Auf einem Teil der Welt-Bühne spielt sich der Alltag von Datenschützern, IT-Sicherheitsbeauftragten und Co. ab.

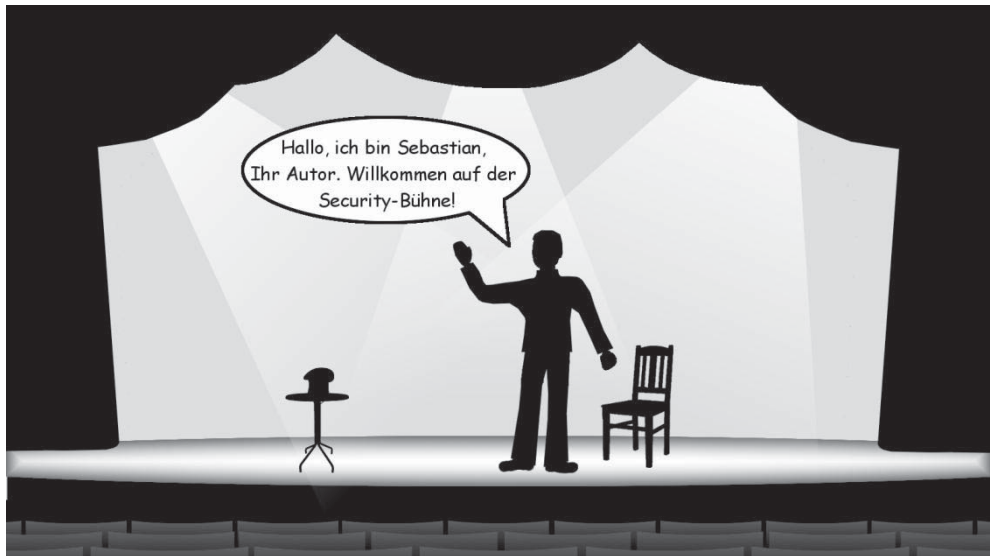


Abbildung 1-1: Willkommen auf der Security-Bühne

Auf dieser Security-Bühne wird ein ganz besonderes Programm geboten: Als zum Beispiel der Datenschutzbeauftragte die Videokameras vor den Werkstoiletten zum ersten Mal sieht, stellt er erschüttert fest: „Ich glaub, ich bin im falschen Film.“ Der Werksleiter, der die Kameras installieren ließ, sagt dazu nur: „Machen sie nicht so ein Theater!“ Der aktuelle Virenvorfall ist „eine Tragödie“: Das ganze Netz ist

---

<sup>5</sup> Erving Goffman; Rahmen-Analyse. Ein Versuch über die Organisation von Alltagserfahrungen; 1996; Suhrkamp; ISBN 978-3518279298

verseucht und auf allen vorhandenen Backup-Datenträgern ist der Virus auch. Für mehr Datenträger war kein Geld da – die Raucherecke musste überdacht werden. Nicht anders sieht es mit der forensischen Untersuchung der Protokolldateien aus: *„Ein Krimi“*.

Auf der Security-Bühne sind die Experten Autor, Regisseur und Titelheld zugleich. Leider arbeiten sie mit Schauspielern zusammen, die ungern Drehbücher lesen und eher auf das Stegreiftheater spezialisiert sind. Alles in allem ergibt sich so ein Schauspiel, bei dem der Regisseur mit auf der Bühne steht und jedem den Text des Stücks hinterhertragen muss. Wir wollen uns im Folgenden ein Beispiel einer solchen Bühne anschauen:

Das Publikum der Security-Bühne ist erlesen. Es besteht neben den Mitarbeitern zum Beispiel aus Security-Redakteuren aller Couleur. Unter ihnen die schärfsten Kritiker, die der Vorstellung ohnehin nur beiwohnen, weil sie über die Schwächen des Stücks berichten wollen. Die Fachzeitschriften und Online-Portale, für die sie arbeiten, berichten nicht über Sicherheit, sondern über Unsicherheit.

Andere wiederum schauen sich das Stück an, um an Informationen zu kommen, die normalerweise hinter den Bühnenaufbauten versteckt sind. Vielleicht plappert einer der Schauspieler die Pointe des nächsten Stücks noch vor dessen Erstaufführung aus.

Einige sind auch nur gekommen um ziellos einige Tomaten in Richtung Bühne zu werfen in der Hoffnung die Handlung zu stören - dann haben die Security-Redakteure wieder was zum Schreiben. Manche Redakteure bezahlen die Tomaten-Werfer sogar dafür. Wieder andere bieten ihre Dienste zum Schutz vor Tomaten-Werfern im Jahres-Abo an. Auch von denen werden die Werfer ab und an finanziell unterstützt.

Ein besonders netter Zuschauer steht mahnend vor dem Orchestergraben und versucht die Akteure darauf hinzuweisen, dass jederzeit jemand das Bühnenlicht ausschalten könnte, weil der Schalter frei zugänglich ist. Da der Security-Held gerade als Regisseur einem Schauspieler den Text zum zehnten Mal erklären muss, hört er von der berechtigten Mahnung nichts. Der Schauspieler, der die Rolle des Geschäftsführers spielt, gibt gerade auf der anderen Seite der Bühne ein Interview. Er berichtet von dem immensen Aufwand, mit dem die Bühnenbeleuchtung modernisiert wurde: *„Damit steht unser Theater an der Weltspitze“*, berichtet er den Reportern voller Stolz und hält den Schumi-Daumen in die Kameras.



**Abbildung 1-2:** Das Chaos auf der Security-Bühne ist fast perfekt

Wenn Sie Security-Experte sind, ahnen Sie, was jetzt passiert: Einer der Tomaten-Werfer trifft mit einem ungezielten Wurf den Schalter: Zack Licht aus! Alle Security-Redakteure im Publikum drücken routiniert auf den rechten Knopf der mitgebrachten Stoppuhr: *„Mal sehen, wie lange es diesmal dauert, bis wieder Licht an ist.“*

Der Geschäftsführer bricht das Interview ab und will sofort *„diesen Security-Heini“* sprechen. Der geprellte Redakteur interviewt den Tomatenwerfer: *„Die sind so doof, ich musste nicht Mal zielen!“* Der Mahner am Orchestergraben verhandelt mit einer Traube heißhungriger Redakteure das Honorar für ein Exklusiv-Interview: *„Ich hatte den Regisseur rechtzeitig vor diesem Fiasko gewarnt.“*

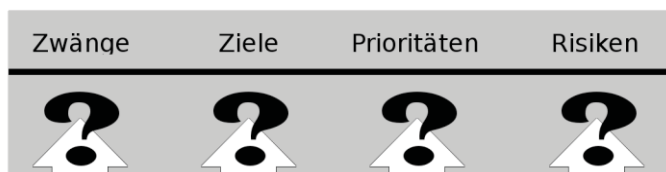
Der Regisseur sitzt mit erschrockenem Gesicht bei dem uneinsichtigen Schauspieler, dem er eben noch zum zehnten Mal den Text vorgesagt hatte. Im trüben Flacker-Licht der Notbeleuchtung sagt dieser zum ersten Mal auch etwas: *„Wofür bekommen sie hier eigentlich ihr Geld, wenn da dauernd das Licht ausgeht.“*

Bei einigen Lesern macht sich jetzt sicher die Erkenntnis breit, dass sie in einem ähnlichen Theater arbeiten – als Regisseur! Aber keine Angst, wie gesagt kommt dem Regisseur auch die Heldenrolle zu. Das gelingt aber nur, wenn er den Überblick behält und genau weiß, welche Stärken und Schwächen seine Protagonisten haben. Wenn er es hinbekommt, dass die Schauspieler auch mal ohne ihn zurechtkommen, kann er den Lichtschalter notfalls persönlich bewachen.

Die Protagonisten sind es gewohnt aus dem Stegreif zu spielen. Damit muss man leben. Es macht keinen Sinn, sie verbiegen zu wollen. Stattdessen macht es Sinn nach einer anderen kommunikativen Ebene zu suchen. Auch wenn es oft für Security-Experten in den Hintergrund tritt: Alle Akteure haben an anderen Bühnen Engagements für Hauptrollen oder sind gar selbst Regisseur. Auf der Security-Bühne treten sie nur nebenbei auf. Die meisten nicht einmal freiwillig – deshalb kennen sie auch nie den Text.

Will der Regisseur nicht zwischen den Akteuren zerrieben werden, muss er sich eingehend mit ihnen auseinandersetzen, sie studieren. Einer der wichtigsten Punkte ist hierbei, sich mit den Hauptrollen auseinanderzusetzen, die sie spielen. Was beschäftigt sie?

Im Grunde muss man sich dieselben Fragen stellen, die sich auch der Vertriebsmitarbeiter stellen muss, um seine Produkte an den Mann oder die Frau zu bringen: Welchen Zwängen unterliegen die Personen des Dramas; welche Ziele verfolgen sie mit welchen Prioritäten? Eine weitere gewichtige Frage ist, welche Risiken sie beunruhigen. Das schätzt nicht jeder gleich ein, weil sich ein konkreter Schadensfall unterschiedlich auf die Betroffenen auswirkt. Die im Sicherheitskonzept beschriebenen Sicherheits-Risiken müssen in Mitarbeiter-Risiken übersetzt werden.



**Abbildung 1-3:** Die vier Problemfelder der Akteure

Im Eingangsbeispiel haben wir bereits die wichtigsten Personen auf der Security-Bühne kennen gelernt. Im Folgenden sollen diese nun genauer unter die Lupe genommen werden. Wir wollen diese Überlegungen beim Management beginnen und uns über die Security-Fachleute zu den Mitarbeitern durcharbeiten. Am Ende werden die Zwänge, Ziele, Prioritäten und Risiken für all diese Gruppen wie eine übersichtliche Landkarte vor uns liegen.

## 1.1 Geschäftsleitung, Behördenleitung und oberes Management

In GmbHS die Geschäftsführer, in AGs die Vorstände, in Behörden die Dienststellenleiter – im Folgenden fassen wir all diese Bezeichnungen unter dem Begriff *Chef* zusammen. Wenn es darum geht die Verantwortlichen zu finden ist

man auf dieser Ebene goldrichtig. Das Leben der IT-Sicherheits- und Datenschutzbeauftragten sollte also ziemlich einfach sein. Leider sind die genannten Akteure wahre Meister darin für Ihre Verantwortung einen Schuldigen zu finden, wenn es zum Schwur kommt. Aber eins nach dem anderen; noch sind wir nicht bei den Konflikten.

Der erste Akteur, den wir näher beleuchten wollen, ist die Diva unseres Ensembles. Den Chef kennt jeder. Immer im Mittelpunkt umgibt ihn eine unnahbare Aura. Einige bezeichnen ihn als abgehoben und launenhaft. Es wurde berichtet, dass er sein persönliches Umfeld schon Mal schikanieren kann, wenn die Tagesform im Keller ist. Seine Hauptrolle spielt er in dem Bühnenstück *Being the Boss*. In den Abteilungen des Unternehmens gibt er nur Gastspiele. Das gilt auch für die Security-Bühne. Die Rolle als *Boss* fordert das ganze Talent und die ganze Hingabe unseres Akteurs. Wenn wir wissen wollen, was ihn umtreibt, dann müssen wir uns mit dieser Rolle auseinandersetzen.

Das Bühnenstück *Being the Boss* beruht auf dem Sachbuch *Gewinnmaximierung und Rentabilitätsmaximierung als Ziel erwerbswirtschaftlich orientierter Unternehmungen und die Erreichung dieses Zieles durch optimalen Einsatz des Eigenkapitals*<sup>6</sup>. Das Buch ist von 1967. Die Lochkartenmaschine IBM 601 ist da schon 32 Jahre alt und Konrad Zuses Z1 steht kurz vor dem 30. Geburtstag. Alles in allem spielte damals die Sicherheit von Unternehmensinformationen eine untergeordnete Rolle. Das hat sich in den meisten Unternehmen bis heute leider nicht geändert.

Der Titel des Buchs aus den Sechzigern ist auch heute noch der Maßstab, an dem sich die Chefs dieser Welt messen lassen müssen. Bei der Erreichung dieses Ziels stehen sie meist alleine da. Die öffentliche Meinung schlägt die erwirtschafteten Gewinne oft der Arbeit der Belegschaft zu. Verluste sind auf mangelndes Management zurückzuführen. Kurz: Chefs haben es nicht leicht. Uns geht es aber nicht darum Mitleid vorzutäuschen. Unsere Neugier richtet sich auf die Beweggründe, die Chefs umtreiben. Wenn wir etwas erreichen wollen, müssen wir uns auf unser Gegenüber einstellen. Dabei ist es uns durchaus erlaubt, aus unserer Sicht an der Sache vorbeizureden, wenn das zum Erfolg führt. Security-Experten reden viel zu oft von der Sache und werden in der Folge nicht richtig verstanden.

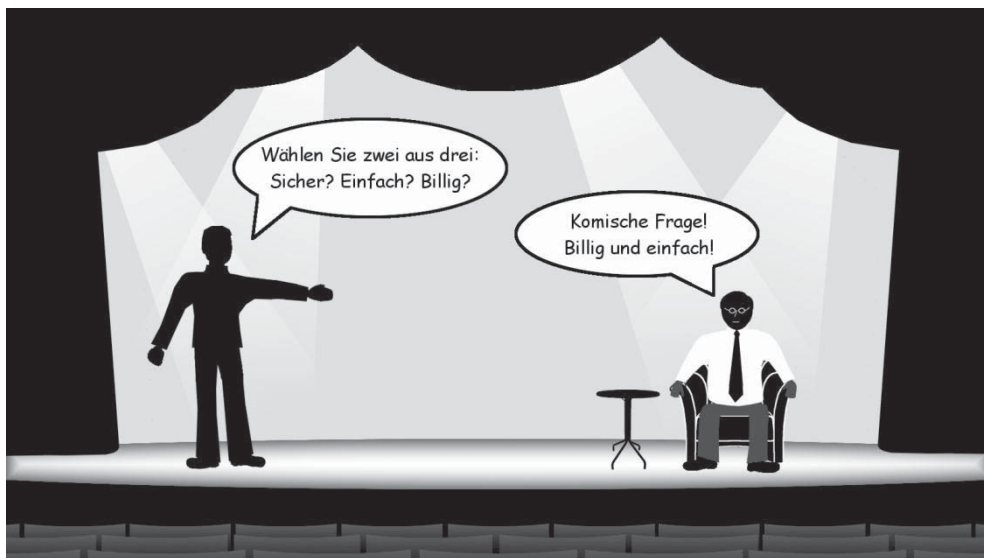
Sie fragen sich vielleicht, was daran falsch sein soll, von der Sache zu reden. Das liegt daran, dass Sie wahrscheinlich selbst Security-Experte sind und zur Sache viel zu sagen haben. Sie kennen Sicherheitsziele; Sie wissen in welcher Reihenfolge sie anzugehen sind und Sie haben genaue Vorstellungen zu den Risiken der

---

<sup>6</sup> Hans-Ferdi Jennihsen; *Gewinnmaximierung und Rentabilitätsmaximierung als Ziel erwerbswirtschaftlich orientierter Unternehmungen und die Erreichung dieses Zieles durch optimalen Einsatz des Eigenkapitals*; 1967; Westdeutscher Verlag; ASIN: B0000BRSM8

modernen Kommunikationstechnik. Die Problemfelder der Security-Bühne sind für Sie ein offenes Buch, das sie frei zitieren. Was für Sie ein offenes Buch ist, ist für Ihren Chef ein Buch mit sieben Siegeln.

Es hilft nichts: Auf diesem Weg kommt man nicht zum Ziel. Selbst wenn, in der Sprache des o.a. Buchs über die Gewinnmaximierung brauchen Sie bestenfalls die Hälfte der Worte. In dessen Nachbarschaft finden Sie auf den Buchrücken in der Bibliothek eine ziemlich genaue Beschreibung der Motive Ihres Chefs. Wenn Sie mit Ihrem Chef sprechen, dann müssen Sie seine Problemfelder ansprechen.



**Abbildung 1-4:** Die Zwei-Aus-Drei-Entscheidung

In Abbildung 1-4 sehen Sie den klassischen Fehler. Was der Sicherheitsexperte fragt, ist auf die Security-Problemfelder zugeschnitten. Der Chef übersetzt die Frage in seine Problemfelder – die Antwort war zu erraten. Ein ähnliches Missverständnis aus dem täglichen Leben spielt sich jeden Samstagnachmittag in deutschen Wohnzimmern ab:

*„Schatz, wollen wir um 18 Uhr zu Heidi und Günther gehen und uns mal den kleinen Felix anschauen? Der kann mittlerweile laufen. Oder willst Du lieber Sportschau sehen?“, fragt Simone ihren Freund Michael.*

*„Sportschau“, lautet Michaels karge Antwort.*

Die Zwänge und Ziele, denen Simone und Michael unterliegen, scheinen nicht deckungsgleich zu sein. Schon gar nicht die Prioritäten! Wenn Simone sich auf Michaels Problemfelder einstellt, kann sie ihre Ziele besser erreichen:

*„Schatz, wollen wir die Sportschau heute bei Heidi und Günther anschauen? Die beiden Grillen und stellen den Breitbildfernseher im Garten auf. Danach könnt ihr Männer mit dem kleinen Felix kicken, der kann nämlich schon laufen.“*

Michaels Antwort lautet diesmal: *„Das hört sich toll an. Machst Du wieder Deinen sensationellen Nudelsalat?“*

Wenn wir also die Antwort auf eine Frage schon kennen, bleibt nur übrig, die Frage anzupassen. Natürlich ist das auf den ersten Blick mit mehr Arbeit verbunden und diese Arbeit geht auch meist am eigentlichen Thema vorbei, aber sie zeigt Wirkung. Simone muss sich mit Heidi zusammentun, ein Grillen planen und einen Nudelsalat machen. Trotzdem: Ziel erreicht.

Kommen wir also zu dem Motiv zurück, das unseren Chef umtreibt: *Gewinnmaximierung und Rentabilitätsmaximierung und die Erreichung dieses Zieles durch optimalen Einsatz des Eigenkapitals*. Auf dieser Grundlage können wir die Problemfelder bestimmen, in denen wir unsere Security-Botschaften ausdrücken müssen. Ganz oben auf der Agenda steht das Ziel *Gewinn- und Rentabilitätsmaximierung*. Zu erreichen ist es durch den optimalen Einsatz des Eigenkapitals. Das ist der äußere Zwang, den die Eigenkapitalgeber dem Chef auferlegen. Aus dem Ziel und dem Zwang leiten sich die Prioritäten ab, nach denen Entscheider vorgehen. Welche Risiken nehmen Chefs also wahr?

Der IT-Sicherheitsbeauftragte Tim steht vor dem Geschäftsführer: *„Chef, auf der Webseite der Bundeswehr sind nach einem Hack zwei schräge Typen abgebildet, die in einem Cabrio durch die Wüste fahren. Über dem Bild steht make love, not war ;) Das könnte uns auch passieren!“*

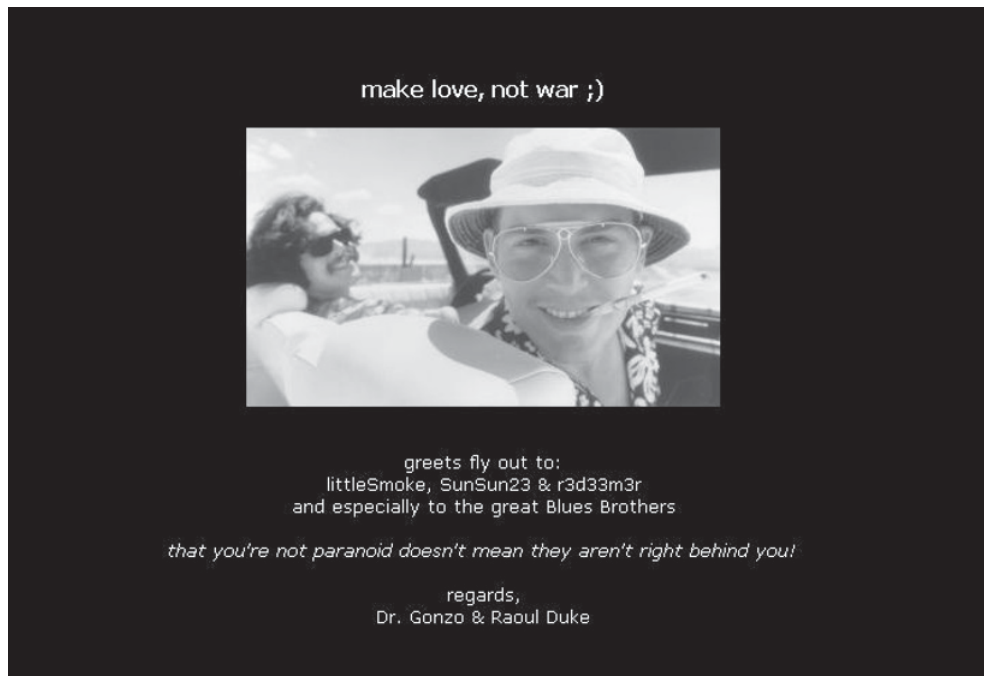
*„Wird es aber nicht“,* sagt der risikofreudige Chef. *„Wir sind nicht die Bundeswehr“,* bemerkt er lachend und das Gespräch ist beendet.

Versuchen Sie es selbst. Versuchen Sie, das von Tim beschriebene Problem in den Problemfeldern des Chefs wirken zu lassen. Vielleicht kommen Sie zu einem ähnlichen Ergebnis wie ich:

*„Chef, unser Kerngeschäft ist gefährdet. Wir stehen dem Problem gegenüber, dass eine Stunde Ausfall unserer Webseite, Bestellungen in fünfstelliger Höhe verhindert. Der Vertrieb geht davon aus, dass auch in diesen kurzen Zeiträumen Kunden dauerhaft verloren gehen. Die Marketing-Abteilung schätzt den Aufwand zur Stabilisierung der Nachfrage nach einem Ausfall von nur einem Tag ebenfalls im fünfstelligen Bereich. Aktuelle Vorfälle führen zu Ausfällen von bis zu drei Tagen. Wenn wir die Absicherung der Webseite geschickt nutzen, könnten wir damit sogar neue Kunden*

*ansprechen. In der Firmenzentrale in den USA sind diese Maßnahmen schon umgesetzt. Auch die Konkurrenz hat sich weitestgehend auf dieses Risiko eingestellt.“*

Das zieht – versprochen! Es zieht, weil es die Risiken aufzeigt, die den Priorität-1-Zielen des Chefs drohen. In den letzten beiden Sätzen wird das Ganze noch mit ein wenig Zwang nachgewürzt und fertig. Wenn die Nebenrolle auf der Security-Bühne für den Chef existenzbedrohend wichtig wird, wenn er denkt er verliert bei schlechter Performance seine Hauptrolle, dann sind Sie auf dem richtigen Weg.



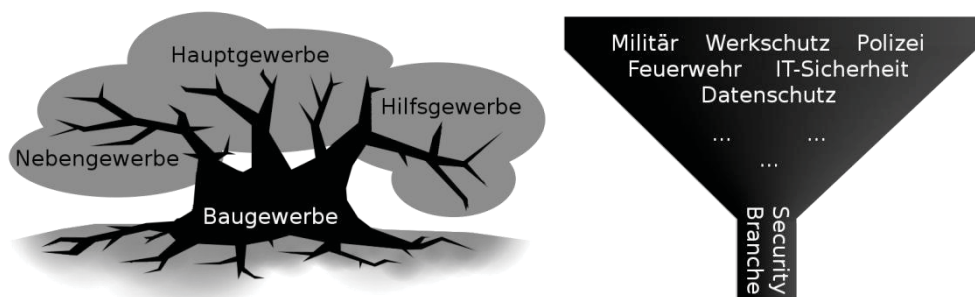
**Abbildung 1-5:** Bundeswehr.de am 19.01.2003. Das gezeigte Bild stammt aus dem Film Fear And Loathing In Las Vegas

Sich der Unterstützung der Chef-Etage zu versichern ist eine der wichtigsten Aufgaben der Sicherheitsexperten, die auf allen ToDo-Listen ganz oben stehen muss. Alle anderen Sicherheits-Maßnahmen werden davon beeinflusst, ob sie vom Chef unterstützt werden. Wenn er selbst das größte Sicherheitsrisiko ist, wird es schwer, Erfolge bei der Stärkung der Sicherheitskultur zu erreichen. Wie man Geschäftsleitung, Behördenleitung und oberes Management für Sicherheit begeistern kann wird in Abschnitt 3.4.2 ausführlich beleuchtet.

## 1.2 Sicherheitsexperten

Bisher haben wir - mit einigem Leichtsinn – von *der* Security-Bühne gesprochen, ganz so als gäbe es einen homogenen, von allen gleich verstandenen Sicherheitsbegriff. Im Gegenteil: Es gibt eine nahezu grenzenlose Fülle von Sichtweisen auf das Thema. Mit dem Schlagwort Sicherheit wird heute so manche Idee verkauft. Die Nuancen und Spezialisierungen, in denen sich die Security-Branche entwickelt hat, sind wenig transparent.

Normalerweise entstehen Spezialisierungen in einem Fachgebiet zur wirtschaftlichen Optimierung von Arbeitsabläufen. Dabei bildet sich eine Baumstruktur des Fachgebiets. Will man sich – ausgehend von dem Wort Sicherheit – einen Branchenbegriff erarbeiten, gerät man schnell ins Straucheln. Sicherheit bezeichnet einen Zustand, der frei von Gefahr ist. Das würde alle Firmen und Institutionen zur Security-Branche hinzurechnen, die sich mit der Abwendung von Gefahren auseinandersetzen. Das erinnert weniger an eine Baumstruktur, als an einen Trichter, in den eine Unzahl loser Begriffe gegossen wird.



**Abbildung 1-6:** Manche Branchen wie das Baugewerbe werden durch Verordnungen<sup>7</sup> gegliedert. In der Security-Branche existiert so eine Systematik nicht.

Das Militär soll die äußere Sicherheit eines Landes garantieren; die Polizei vertritt die Innere Sicherheit; Arbeitssicherheit, Feuerwehr und Werkschutz; IT-Sicherheit, Datenschutz etc. Selbst der Schlosser, der mit seinem Schlüsseldienst unzählige Wohnungstüren sicherer gemacht hat, gehört der Security-Branche an.

In Unternehmen und Dienststellen der Öffentlichen Verwaltung werden Security-Spezialisierungen durch eine Reihe von Experten repräsentiert. Welche das im Einzelnen sind, weicht teilweise erheblich voneinander ab. Drei Funktionen haben sich jedoch herauskristallisiert, die sich gut unterscheiden lassen:

<sup>7</sup> Baubetriebe-Verordnung vom 28. Oktober 1980 (BGBl. I S. 2033), zuletzt geändert durch die Verordnung vom 26. April 2006 (BGBl. I S. 1085) ↗

- ❖ Zunächst haben wir die Sicherheitsbeauftragten. Die Akteure auf der Security-Bühne der klassischen Unternehmens- und Behördensicherheit sind gut eingespielt. Zu Zeiten des Kalten Kriegs liefen sie zur Hochform auf, auch wenn manch einem das Programm heute ein wenig verstaubt erscheint. Wachschutz, Spionageabwehr und Sicherheitsüberprüfung sind die passenden Schlagworte.
- ❖ Eine zweite Gruppe bilden die Datenschutzbeauftragten. Die Datenschutzgesetze machen es uns in diesem Fall einfach, den Tätigkeitsbereich abzugrenzen. Die gesetzlichen Regelungen sind der Text, nach dem auf der Security-Bühne der Datenschützer gespielt wird.
- ❖ Für die dritte Gruppe von Sicherheitsbeauftragten stehen Informationssysteme und die mit ihnen verarbeiteten Informationen im Mittelpunkt. Eine ganze Reihe von Stellenbezeichnungen müssen hier eingeordnet werden. Hierzu gehören IT-Sicherheitsbeauftragte, CISOs (Chief Information Security Officers) oder auch Informationssicherheitsbeauftragte.

Wir wollen nun diese drei Spezialisierungen näher betrachten. Die Personen die diese Funktionen wahrnehmen treten jeweils in der Rolle als Regisseur und Held der Security-Bühne in Erscheinung – in vielen Fällen zu dritt auf einer Bühne:



**Abbildung 1-7:** Viele Köche verderben den Brei: Datenschutz, IT-Sicherheit und klassische Unternehmenssicherheit dürfen sich nicht gegenseitig übertrumpfen oder konkurrieren.

Wie schon im Abschnitt Geschäftsleitung, Behördenleitung und oberes Management wollen wir auch hier fragen, durch welche Zwänge und Ziele die

drei Akteure gesteuert werden, welche Prioritäten sie setzen und welche Risiken für sie wichtig sind. Wir werden sehen, dass diese bei den unterschiedlichen Sicherheitsexperten nicht gleich sind. Vielmehr muss man sich die Problemfelder als Scheiben vorstellen, die sich nur teilweise überdecken. So entsteht ein Spiegel der Unternehmens- oder Behördensicherheit. Manche Bereiche werden von allen drei angegangen, bei anderen Dingen stehen sie alleine da.

### 1.2.1 Sicherheitsbeauftragte

Seit Sicherheit organisiert werden muss, gibt es Sicherheitsbeauftragte. Schon zur Zeit des Pharaos Ramses IX (1127/1128 bis 1100 v. Chr.) gab es für das Tal der Könige einen Sicherheitsbeauftragten. Pawero hatte mit einer wahren Plage von Grabräubern zu kämpfen. Plünderungen der Gräber waren damals sehr beliebt, besonders, weil man sich durch Bestechung mit der Beute freikaufen konnte. Der Fall des Grabräubers Amenpanufer verlief jedoch anders<sup>8</sup>: Unter Folter offenbarte er das ganze Ausmaß der Korruption. Zahlreiche Wachen, Beamte und Kaufleute wurden so überführt und hingerichtet. Die Geschichte sollte jedoch zeigen, dass Pawero – der „*Getreue des Pharaos*“ – an der Spitze der Bande stand. Wir kommen später darauf zurück, wie wichtig es ist, Interessenkonflikte zu vermeiden.<sup>9</sup>

Etwas später, zur Zeit des Kaisers Qin Shiuangdi (Ende des 3. Jahrhunderts v. Chr.) waren General Meng-tian und sein Beraterstab mit der Konzeptionierung der Sicherheit beauftragt.<sup>10</sup> Ihre Hauptaufgabe: Der Bau der Chinesischen Mauer zum Schutz vor Angreifern aus dem Norden. Mehr als 1000 Jahre später wurde den Chinesen der Ausbau der Mauer zu teuer. Nachdem man sich ihrer Sicherheit nicht mehr mit der nötigen Aufmerksamkeit widmete, wurde sie auch recht bald überwunden.

Ob im alten Ägypten Pawero oder zu Zeiten des Kaisers Qin Shiuangdi General Meng-tian und sein Beraterstab – sie alle steuerten die Sicherheitsanstrengungen ihrer Zeitgenossen. Über Jahrtausende ging es um greifbare, mechanische Sicherheitsbegriffe: Je dicker die Tür, je komplizierter das Schloss, je mehr Wachen, desto größer war der Schutz vor äußerer Gefahr. Aber auch der Schutz vor der Gefahr von innen – vor Verrat – musste gewährleistet werden.

Damals wie heute sind das die Schwerpunkte der klassischen Sicherheitsbeauftragten. Wie dick die Tür sein muss, wird heute in

---

<sup>8</sup> Pascal Vernus; *Affairs and Scandals in Ancient Egypt*; 2003; Cornell University Press; ISBN 978-0801440786; Seite 5 ff

<sup>9</sup> Siehe Abschnitt 2.4 - Interessenkonflikte

<sup>10</sup> Julia Lovell; *Die Große Mauer: China gegen den Rest der Welt. 1000 v. Chr. – 2000 n. Chr.*; 2007; ISBN 978-3-8062-2074-2; Seite 52 ff

Widerstandsklassen angegeben, Schließzylinder werden nach Angriffswiderstandsklassen<sup>11</sup> sortiert und auch in der Gebäudebewachung setzt man auf modernere Taktiken und – mehr und mehr – auf Technik.

Die Probleme der Sicherheitsbeauftragten sind seit jeher die gleichen: Wenn die Burg längere Zeit nicht von Raubrittern überfallen worden ist, wird das Budget für die Wachen gekürzt; wurde lange nichts gestohlen, werden die Türen nicht mehr abgeschlossen. Was Verantwortliche und Betroffene mit der Zeit vergessen: Die Raubritter wurden abgeschreckt, weil die Burg so gut bewacht war und die Diebe sind wegen der verschlossenen Türen fern geblieben – es gab ja nichts zu holen.

An diesen Beispielen lässt sich ein Phasenverlauf ablesen, anhand dessen deutlich wird, wann dem Sicherheitsbeauftragten Konflikte drohen. Auf der klassischen Security-Bühne wird in zwei Akten gespielt. Der erste Akt heißt *Panik*, der zweite Akt *Rückfall*. Die Handlung spielt in jeweils drei Szenen.

|                          |           |            |          |
|--------------------------|-----------|------------|----------|
| <b>1. Akt „Panik“</b>    | Naivität  | Vorfall    | Angst    |
| <b>2. Akt „Rückfall“</b> | Maßnahmen | Beruhigung | Naivität |

**Tabelle 1-1:** Das Security-Storyboard

## **1. Akt: Panik**

### **1. Szene: Naivität**

Man könnte die Eingangsszene auch mit den Worten *Friede – Freude – Eierkuchen* überschreiben. Das ist die Phase, in der eine drohende Gefahr noch unbekannt ist. Niemand rechnet damit, dass etwas passieren könnte. Der Sicherheitsbeauftragte hat seinen Auftritt erst im zweiten Akt.

### **2. Szene: Vorfall**

In der zweiten Szene werden die Beteiligten durch einen Vorfall aus ihrem Dornröschenschlaf gerissen. Was nicht sein konnte ist nun doch passiert. Der Angriff auf das World Trade Center in New York am 11.09.2001 war ein solches Ereignis, mit dem niemand gerechnet hatte.

### **3. Szene: Angst**

In der dritten Szene setzt sich die Erkenntnis durch, dass man von Anfang an viel zu naiv war. Nach dem ersten Schock steht fest: Was ein Mal passieren

---

<sup>11</sup> U.a.: DIN V ENV 1627 und DIN 18252 - Profilzylinder für Türschlösser 

kann, kann sich jederzeit wiederholen. Angst macht sich breit und die Katastrophen-Phantasien erreichen ungeahnte Ausmaße.

## **2. Akt: Rückfall**

### **4. Szene: Maßnahmen**

Der erste Akt endete in Panik und Ratlosigkeit. Zu Beginn des zweiten Akts ruft jeder nach Orientierung und einem Retter in der Not. Der Sicherheitsbeauftragte ist der Mann der Stunde. Seine Maßnahmen zur Gefahrenabwehr werden von Allen beklatscht und euphorisch gefeiert. Niemand fragt nach – warum auch – man ist in dem Ziel vereint, dass sich die 2. und 3. Szene nicht wiederholen mögen.

### **5. Szene: Beruhigung**

Die Maßnahmen zeigen Wirkung. Kausal oder nicht, steht hier nicht zur Debatte. In vielen Hollywood-Filmen ist das die Schluss-Szene<sup>12</sup>. Das ist auch sinnvoll, weil die 5. Szene die schönste ist – alle sind zufrieden. In der Realität der Security-Bühne sieht es aber anders aus.

### **6. Szene: Naivität**

In der 6. Szene fallen die Akteure wieder in den alten Trott zurück. Der Vorfall gerät in Vergessenheit und man fragt den Sicherheitsbeauftragten, ob er es mit den Maßnahmen nicht ein wenig übertrieben hat. Die 6. Szene findet man in Hollywood-Filmen höchstens als 1. Szene von Teil II<sup>13</sup>.

Für Sicherheitsbeauftragte ist die 6. Szene der alltägliche Wahnsinn. Für die meisten dürfte der Eindruck vorherrschen, dass sie dauerhaft in Szene 6. festhängen und nur ab und an eine Schleife über die Szenen 2. bis 5. einlegen, die die Akteure in Windeseile durchschreiten, um mit großer Beharrlichkeit an Szene 6. zu feilen.

Nehmen Sie die historischen Beispiele vom Beginn dieses Abschnitts – auf der Security-Bühne wird schon immer nach einem ähnlichem Storyboard gespielt: Aus der Naivität über einen Vorfall zurück in die Naivität. Security war immer schon zu einem bedeutenden Teil durch Vorfälle gesteuert. Die Maßnahmen sorgen aber

---

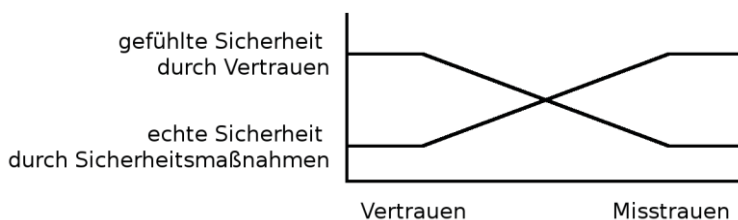
<sup>12</sup> Manchmal werden aus dramaturgischen Gründen die Szenen 2 – 5 noch einmal im Schnelldurchlauf wiederholt. Zum Beispiel ist der falsche Täter inhaftiert worden und der richtige mordet weiter.

<sup>13</sup> Z.B.: Alien I-IV – Obwohl sich alle sicher waren: Das Alien war immer zu Beginn des nächsten Teils doch nicht tot.

dafür, dass es keine Vorfälle mehr gibt und es ergibt sich die aufgezeigte Wellenbewegung.

Im Verlauf dieser Wellenbewegung verändern sich die Ziele der Sicherheitsbeauftragten kaum. Was sich ändert, sind die äußeren Zwänge, die auf sie einwirken. Ist das Angst-Erlebnis noch frisch, wird nach harten Maßnahmen gerufen. Wenn Verantwortliche und Mitarbeiter den Grund für die Maßnahmen langsam vergessen, kehrt sich dieser Zwang ins Gegenteil und die Sicherheitsbeauftragten müssen die Maßnahmen verteidigen, die vor einiger Zeit noch mit Vehemenz eingefordert wurden. Die Akteure werden dabei von Ihrem Inneren gesteuert. In ihrer Angst reagieren sie mit Misstrauen.

Der Mensch sehnt sich nach Vertrauen und hat eine instinktive Ablehnung gegen Maßnahmen, die Misstrauen ausdrücken. Das Gefühl des Vertrauens wird als freundlich und sicher empfunden. In einer feindlichen Umgebung, in der es an Vertrauen fehlt, fühlt man sich unsicher und ausgesetzt.<sup>14</sup> Bei allen Sicherheitsmaßnahmen muss dieser Sachverhalt berücksichtigt werden: Die gefühlte Sicherheit verläuft genau entgegen der tatsächlichen Sicherheit.



**Abbildung 1-8:** Die gefühlte Sicherheit verläuft entgegen der tatsächlichen Sicherheit

Wir werden uns mit dieser Problematik in Abschnitt 2.5 beschäftigen. Sie ist verantwortlich für manches Missverständnis zwischen Sicherheitsbeauftragten und ihrer Umgebung. Mit der richtigen Kommunikationsstrategie kann dieser naturgemäße Kurvenverlauf positiv beeinflusst werden.

### 1.2.2 Datenschutzbeauftragte

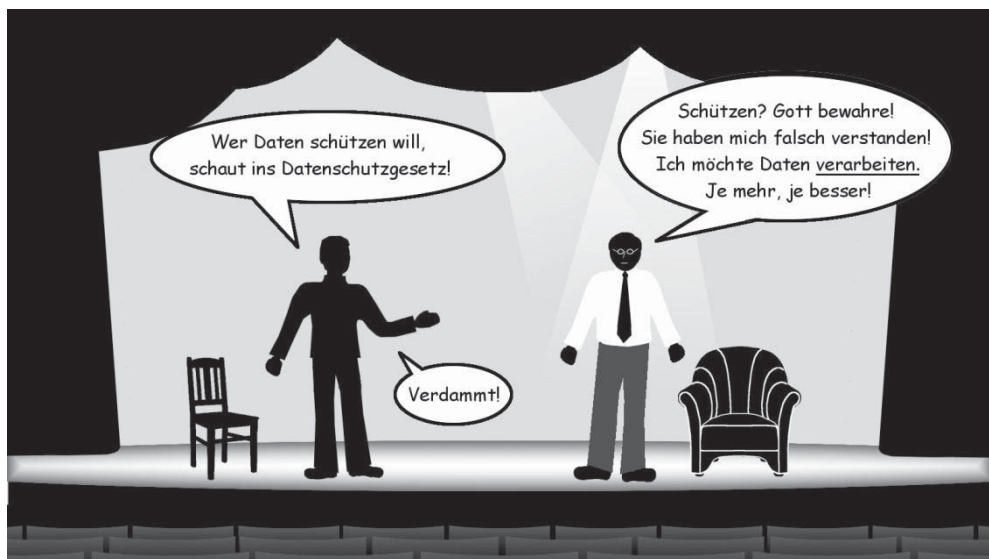
Die Geschichte des Datenschutzes ist, verglichen mit der langen Historie der klassischen Sicherheitsbeauftragten, noch jung. Der Begriff selbst wurde in seiner heutigen Bedeutung erst in den 70er Jahren des letzten Jahrhunderts geprägt.

<sup>14</sup> Martin Hartmann, Claus Offe (Hrsg.); Vertrauen. Die Grundlage des sozialen Zusammenhalts; 2001; Campus Fachbuch; ISBN 978-3593367354; Seite 86

Wenn man das Dilemma der Datenschutzbeauftragten ergründen will, muss man zuerst der Frage nach dem Ursprung des Datenschutzes auf den Grund gehen. Während die klassischen Sicherheitsbeauftragten die Organisation selbst schützen, der sie dienen, schützen die Datenschutzbeauftragten die Beteiligten vor der Organisation. Sicherheitsbeauftragte sorgen also für die äußere Sicherheit der Gemeinschaft und Datenschutzbeauftragte für die Freiheit des Individuums innerhalb der Gemeinschaft.

Bei ihrer Arbeit stützen sie sich auf Datenschutzgesetze. Wenn man so will, sind Datenschutzbeauftragte in gewisser Weise privatisierte Vollzugsbeamte. Sie dienen nicht dem Unternehmen oder der Behörde, der sie angehören, sondern den einschlägigen Datenschutzgesetzen.

Es gibt Gesetze, die sollen klären, wie etwas sein soll und solche deren Ziel es ist festzulegen, wie etwas nicht sein soll. Die Datenschutzgesetze gehört in die zweite Gruppe von Gesetzen – zumindest in der Wahrnehmung vieler Akteure. Warum ist das so? Diese Wahrnehmung geht auf das zentrale Missverständnis zurück, das vielen unterläuft: Wer einen Verein gründen will, schaut im Bürgerlichen Gesetzbuch auf die §§ 21 ff und erfährt, was er zu tun hat<sup>15</sup>.



**Abbildung 1-9:** Zielkonflikt: Daten schützen oder verarbeiten?

<sup>15</sup> Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das durch Artikel 4 Absatz 10 des Gesetzes vom 11. August 2009 (BGBl. I S. 2713) geändert worden ist"

Wer Daten schützen will muss ins Datenschutzgesetz schauen. Genau: „Wer Daten *schützen* will...“ Wer hingegen Daten *verarbeiten* will, muss einsehen, dass es sich beim Datenschutzgesetz nicht um ein *Datenverarbeitungsgesetz* handelt.

Die Security-Bühne der Datenschutzbeauftragten spielt Tragödien nach dem Muster: „*Zwei Seelen wohnen, ach! in meiner Brust.*“<sup>16</sup> Wer in dieser Situation bestehen will, kommt nicht umhin, es Goethes Faust gleichzutun und zu Beginn der Tragödie auf diesen Sachverhalt hinzuweisen. Datenschutzbeauftragte gibt es in Unternehmen und Behörden nicht, weil Chefs das so wollen - Sie sind von Gesetzeswegen schlicht dazu gezwungen. Das macht sich natürlich im Zusammenspiel mit allen Akteuren der Security-Bühne bemerkbar. Was dem klassischen Sicherheitsbeauftragten von seinen Chefs noch *von Herzen* abverlangt wird – z.B. die Absicherung des Warenlagers gegen Einbrecher – wird vom Datenschutzbeauftragten nur halbherzig gefordert. Der genaue Wortlaut des Gesetzes wird nur widerwillig angehört. Viele Chefs erwarten sich von ihren Datenschutzbeauftragten eher vertiefte Kenntnisse in den Gesetzeslücken statt in den dort aufgeführten Geboten.

Die Aufgabe, von den Problemfeldern des Datenschutzbeauftragten in die Problemfelder des Chefs zu übersetzen ist besonders schwierig. Die Ziele des Datenschutzbeauftragten zu ermitteln fällt noch relativ leicht: Man kann sie fast eins zu eins aus den Gesetzen ablesen. Leider sind die Abweichungen zu den Zwängen teilweise immens. Die Zwänge wirken von außen und entsprechen jeweils einer Teilmenge aus den Zielen der anderen Akteure. Beim klassischen Sicherheitsbeauftragten sind diese Zwänge noch relativ homogen: Dass niemand ins Warenlager einbricht, ist in aller Interesse. Es gibt keine echten Gegenredner zu diesen Zielen. Die Zwänge, die man dem Sicherheitsbeauftragten auferlegt spielen ihm also meistens in die Karten.

Der Datenschutzbeauftragte muss mit einem ganzen Strauß an Zwängen zurechtkommen, die alle eine unterschiedliche Stoßrichtung aufweisen. Nehmen wir folgendes Beispiel, dass sich an einen Fall aus dem Forum des Bundesdatenschutzbeauftragten anlehnt<sup>17</sup>:

In der Verwaltung eines Kaufhauses hat eine neue Auszubildende ihre Lehrstelle angetreten. Nennen wir sie Julia Schneider. Von der Belegschaft war der Wunsch aufgekommen, dass neue Kollegen in irgendeiner Form im Kreise der Belegschaft vorgestellt würden. Der Vorgesetzte von Frau Schneider sagt ihr deshalb, sie solle

---

<sup>16</sup> Johann Wolfgang Goethe; Faust – Der Tragödie erster Teil; 1986; Reclam; ISBN 3-15-000001-7; Seite 33; Vers 1112

<sup>17</sup> [http://www.bfdi.bund.de/bfdi\\_forum/showthread.php?t=470](http://www.bfdi.bund.de/bfdi_forum/showthread.php?t=470); eingesehen am 06.09.2009; archiviert unter <http://www.webcitation.org/5jaUad7Rr> (Namen und Personaldaten des Beispiels sind frei erfunden)

sich per Mail vorstellen, am besten mit Bild im Anhang. Daraufhin verfasst sie die folgende Mail:

*„Liebe Kollegen,*

*mein Name ist Julia Schneider, ich habe gestern meine Ausbildung als Einzelhandelskauffrau begonnen. Ich möchte mich kurz bei Ihnen vorstellen:*

*Ich bin 16 Jahre alt und komme aus Hannover. Im Juli 2009 habe ich die Realschule erfolgreich beendet. Meine Hobbies sind Handball und Lesen...“*

Als Anhang wird ein Bild von Frau Schneider angehängt, das ihr Vorgesetzter noch schnell von ihr gemacht hat. Eigentlich sind alle zufrieden – niemand beschwert sich. Uneigentlich muss der Datenschutzbeauftragte jedoch die Gesetzeslage im Auge behalten und den Finger in die Wunde legen. Frau Schneiders Vorgesetzten muss er fragen, ob sie der Datenverarbeitung zugestimmt hat. Der wird erwidern, dass sie die Mail doch selbst geschrieben habe, woraufhin der Datenschutzbeauftragte sagt, dass diese Einverständniserklärung nicht den Anforderungen des Datenschutzgesetzes genüge. Frau Schneider ist das alles egal. Sie sagt, sie habe das mit dem Bild zwar nur gemacht, weil sie der Chef dazu aufgefordert habe, aber nun sei die Mail ja schon raus und nichts mehr zu machen. Jetzt schaltet sich der Betriebsrat ein und fordert, dass in dem Fall gegen den Vorgesetzten vorgegangen wird, weil dieser eine unrechtmäßige Datenverarbeitung angeordnet habe und informiert die Chefin des Kaufhauses. Diese will sofort den Datenschutzbeauftragten sprechen und wissen, was der ganze Käse soll: *„Niemand hatte hier ein Problem, bis sie angefangen haben, so lange zu bohren, bis jemand ein Problem hatte.“* Frau Schneider wird das alles mehr und mehr peinlich – so hatte sie sich den Schutz ihrer Daten nicht vorgestellt. Das Ergebnis lautet: Der Datenschutzbeauftragte macht seine Arbeit und alle sind unzufrieden!

Als Datenschützer muss man diese Reaktionen gedanklich vorwegnehmen und sie mit den richtigen Kommunikationsstrategien abfangen, damit die Tragödie doch noch ein Happy-End bekommen kann. Wir werden uns mit dieser Herausforderung in den weiteren Kapiteln auseinandersetzen.

### 1.2.3 IT-Sicherheitsbeauftragte

Auch die Funktion der IT-Sicherheitsbeauftragten ist im Vergleich zur klassischen Sicherheit noch recht jung. Während der Datenschutz seinen Ursprung in den Personalabteilungen hat, ist die IT-Sicherheit in den IT-Abteilungen entstanden. IT-Sicherheitsbeauftragte sind daher eher technisch geprägt. Mehr und mehr wandelt sich der Begriff IT-Sicherheit jedoch in Richtung Informationssicherheit oder Informationssystemsicherheit. Hieß die Zeitschrift <kes> noch bis 2003 im

Untertitel *Zeitschrift für Kommunikations- und EDV-Sicherheit*, so lautet dieser mittlerweile *Zeitschrift für Informations-Sicherheit*.<sup>18</sup>

Diese Entwicklung bleibt nicht ohne Folgen auf der Security-Bühne: Das Bühnenprogramm für die IT-Sicherheitsbeauftragten wird seit einigen Jahren überarbeitet und umfassend erweitert, obwohl der Name des Stücks gleich geblieben ist, ganz wie bei der Zeitschrift <kes>. Das bietet Raum für Missverständnisse und daraus folgenden Konflikten.

Zu den technischen Aspekten der Sicherheit von Netzwerken und Computern sind Fragen der Prozessmodellierung oder des Risikomanagements hinzugekommen. Damit mischen sich mehr und mehr IT-Sicherheitsbeauftragte in Aufgaben der Linienorganisation und fremde Fachgebiete ein. Von vielen Akteuren wird das als Kompetenzüberschreitung wahrgenommen. Diese Begriffsproblematik wird uns noch im Kapitel 3.2 beschäftigen.

Wenn wir uns mit den Problemfeldern der IT-Sicherheitsbeauftragten befassen wollen, müssen wir diesen Etikettenschwindel im Hinterkopf haben. Wenn auf der Security-Bühne des IT-Sicherheitsbeauftragten der IT-Grundschutz des BSI<sup>19</sup> aufgeführt wird, dann wird der Rahmen deutlich überschritten, den der Begriff IT-Grundschutz vorgibt. Auf den Webseiten des BSI finden wir die Erklärung, was der IT-Grundschutz ist: „*Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit.*“<sup>20</sup> Kein Wort von Technik – aus IT wird I!

IT-Sicherheitsbeauftragte müssen ihre Ziele also besonders klar darlegen – am besten gleich zu Beginn der Vorführung als eine Art Vorspiel. Der Titel des Bühnenstücks muss vorbereitet, übersetzt und in einen Kontext gestellt werden, damit alle Akteure sich gedanklich auf dasselbe Ziel ausrichten. Wer soll denn sonst erraten, dass mit IT nicht nur Informations-Technik gemeint ist sondern deutlich mehr.

Jetzt denken Sie vielleicht, dass es doch nicht verkehrt sein kann, wenn man mehr bekommt als versprochen. Dann stellen Sie sich doch bitte vor, Sie kaufen im Supermarkt eine Packung Spiralnudeln und müssen zuhause feststellen, dass nicht

---

<sup>18</sup> Norbert Luckhardt; Editorial - Rückblick voraus; in: <kes>. Nr. 1, März 2009, ISSN 1611-440X, S. 3-6 ☞

<sup>19</sup> IT-Grundschutz-Standards des Bundesamts für Sicherheit in der Informationstechnik: 100-1 Managementsysteme für Informationssicherheit; 100-2 IT-Grundschutz-Vorgehensweise; 100-3 Risikoanalyse auf der Basis von IT-Grundschutz; 100-4 Notfallmanagement ☞

<sup>20</sup> [https://www.bsi.bund.de/cln\\_155/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards\\_node.html](https://www.bsi.bund.de/cln_155/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html); eingesehen am 06.09.2009; archiviert unter <http://www.webcitation.org/5jaUPy2ci>

nur Spiralnudeln in dieser Packung sind, sondern auch Penne, Bandnudeln und Reis. Als Sie die Nudeln im Supermarkt reklamieren wollen, sagt man Ihnen, das sei alles kein Problem, Sie hätten nur die Spiralnudeln bezahlt, der Rest sei kostenlos mit dabei. Ich denke, Sie wären mit dieser Antwort nicht zufrieden, weil *mehr* eben doch nur bedingt *besser* ist.



**Abbildung 1-10:** Missverständnisse vermeiden

Auch wenn der IT-Sicherheitsbeauftragte weiß, was gemeint ist, so ist es für ihn von ebensolcher Bedeutung, ob es alle anderen Akteure auch verstanden haben. Er spielt ja nicht alleine auf der Security-Bühne. Im Gegenteil, er muss sogar Regie führen über das Zusammenspiel der anderen. Auch hier gilt: Der Empfänger macht die Botschaft. Wenn wir uns also den Chef als beispielhaften Empfänger herausnehmen: Glauben Sie, dass er sich auch nur zwei Tage merken kann, was der Unterschied zwischen IT-, IV-, IS- und I-Sicherheit<sup>21</sup> ist? Die Begriffe werden ja nicht einmal in der Fachliteratur einheitlich verwendet.

Wenn der IT-Sicherheitsbeauftragte als Regisseur auf der Security-Bühne bestehen will, so muss er den Begriff IT-Sicherheit am besten immer übersetzen. Egal mit wem er spricht: Die meisten werden sonst Sicherheit von Computern, Servern und Netzen verstehen, obwohl Sicherheit von Informationen, Business Continuity, Incident Management oder Forensik gemeint ist. Überall, wo man die Neigung

<sup>21</sup> Wenn Sie mit den Abkürzungen auch Schwierigkeiten haben, möchte ich Ihnen kurz beim Erinnern helfen: IT=Informationstechnik, IV=Informationsverarbeitung, IS=Informationssystem, I=Information.

verspürt, den allgemeineren Begriff IT-Sicherheit zu verwenden, muss man nach dem treffenderen Begriff suchen, damit die Akteure verstehen, um was es konkret geht.

Die IT-Sicherheitsbeauftragten müssen sich zu dieser sprachlichen Disziplin selbst zwingen und sich die Zeit nehmen, ihr Thema besser zu erklären. Niemand weiß so gut wie sie, dass der Mensch als Sicherheitsrisiko dominiert und daher besonderer Pflege bedarf. Ein einziger unkooperativer Mitarbeiter ist in der Lage immense technische Sicherheitsbudgets ad absurdum zu führen. Auf der Security-Bühne des IT-Sicherheitsbeauftragten werden alle technischen Raffinessen aufgeboten, die es für Geld zu kaufen gibt. Sie kennen das damit verbundene Problem aus dem Kino: Die schönsten Special Effects bringen nichts, wenn die Schauspieler das Niveau nicht halten können.

Das hat auch Auswirkungen auf die Prioritäten und Risiken, die den IT-Sicherheitsbeauftragten beschäftigen. Das größte Risiko, dass einem reibungslosen Auftritt droht sind die menschlichen Schwächen. Nicht selten wird der Fokus in der täglichen Arbeit aber auf die Technik gelegt. Für IT-Sicherheitsbeauftragte ist das bekannte Terrain – gewissermaßen eine Flucht in einfache Tätigkeiten. Bevor man sich an die Arbeit macht, den Mitarbeitern ihre Security-Marotten auszutreiben, kümmert man sich lieber nochmal um die Regelsätze der Firewalls.

Bisher funktioniert diese Flucht auch ganz gut. Der angesprochene Etikettenschwindel zeigt seine Wirkung auch bei Schuldzuweisungen: In den seltensten Fällen werden IT-Sicherheitsbeauftragte für menschliches Versagen im Zusammenhang mit einem Informationsverlust verantwortlich gemacht und gefragt, was sie gegen menschliches Fehlverhalten unternommen hätten. Würden Sie Informationssicherheitsbeauftragte heißen, wäre das schon nicht mehr so einfach. Aus Sicht des Unternehmens ist das natürlich fatal. Geht es doch nicht darum, hinterher jemanden zur Verantwortung ziehen zu können, sondern darum, Vorfälle von vornherein zu verhindern.

Der Trend weg von der IT-Sicherheit hin zur Informationssicherheit wirkt sich bisher wenig auf Positionsbeschreibungen und die Arbeit aus. Während es hunderte von Büchern zu den technischen Aspekten von Informationssicherheit gibt, gibt es bestenfalls eine Hand voll Bücher, die sich mit der menschlichen Komponente auseinandersetzen.<sup>22</sup> Der Umgang mit den beteiligten Menschen ist jedoch auf der Security-Bühne von entscheidender Bedeutung. Auch hier hilft der Kino-Vergleich: Mit guten Schauspielern kommt man auch ohne technische

---

<sup>22</sup> Beispielsweise das derzeit einzige umfassende deutsche Buch zum Thema Security Awareness: Pokoyski, Dietmar / Helisch, Michael (Hrsg.); Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung; 2009; ISBN: 978-3-8348-0668-0

Spielereien sehr weit. Das bedeutet, der Mensch muss im Mittelpunkt jeder IT-Sicherheitsbetrachtung stehen.

### 1.2.4 Die drei Musketiere

Nachdem wir nun einen Blick auf die Security-Bühne von drei spezialisierten Sicherheitsexperten geworfen haben, haben wir die Möglichkeit, zu fragen, welche Gemeinsamkeiten und Unterschiede es gibt. Auch gilt es zu fragen, ob sie nicht sogar alle auf einer Bühne stehen und sich gegenseitig unterstützen können. Vielleicht stehen sie sich aber auch gegenseitig im Weg?

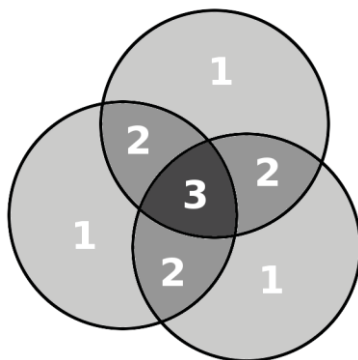


**Abbildung 1-11:** Gemeinsam erreicht man mehr

Fangen wir mit der einfachen Frage an, ob sich die Sicherheitsbemühungen addieren. Abbildung 1-7 von Seite 14 jedenfalls lässt vermuten, dass dem nicht so ist. Addieren können sich Ihre Bemühungen nur da, wo sie sich nicht gegenseitig beeinflussen. Also da, wo jeder für sich selbst an der Sicherheit arbeitet. Stellt man diesen Sachverhalt als Kartoffeldiagramm dar, sind das die in Abbildung 1-12 mit einer 1 gekennzeichneten Bereiche.

Bereiche mit 1 können wir als die unabhängigen Bereiche bezeichnen. Schwieriger wird es zu bewerten, ob sich in den Bereichen 2 und 3 eine Addition ergibt. Im besten Fall wäre es so: In einer perspektivischen Darstellung würden die Schnittflächen der Kreise zur Mitte hin anwachsen. Im schlechtesten Fall behindern sich die drei so sehr, dass es bei den thematischen Schnittmengen zu keinen Ergebnissen kommt. So könnten sich beispielsweise Sicherheit, Datenschutz und

IT-Sicherheit bei der Erarbeitung einer Betriebsvereinbarung zur Protokolldatenauswertung gegenseitig behindern oder sogar blockieren. Genauso gut können sich ihre Bemühungen vollständig ergänzen. Beispielsweise wenn sie gemeinsam von der Geschäfts- oder Behördenleitung fordern, sich für Sicherheitsfragen verantwortlich zu fühlen und das nach außen hin deutlich zu zeigen.



**Abbildung 1-12:** Kartoffeldiagramm der Sicherheit. 1: unabhängiger Bereich 2: bedingt unabhängiger Bereich 3: vollständig abhängiger Bereich

Es ist wichtig, sich darüber Klarheit zu verschaffen, ob man wie die drei Musketiere an einem Strang zieht oder eher dem Bild von drei Parteien im Wahlkampf ähnelt: Alle wollen mehr Sicherheit, aber bestimmt nicht auf dem Weg, den die anderen vorgeschlagen haben. Eine Möglichkeit dies zu tun ist es, sich für die eigene Situation ein Kartoffeldiagramm der Sicherheit anzufertigen. Dazu sind nicht weniger als vier Diagramme nötig: Eines für jedes Problemfeld (Ziele, Zwänge, Prioritäten, Risiken), so wie wir sie in Abbildung 1-3 auf Seite 8 kennengelernt haben.

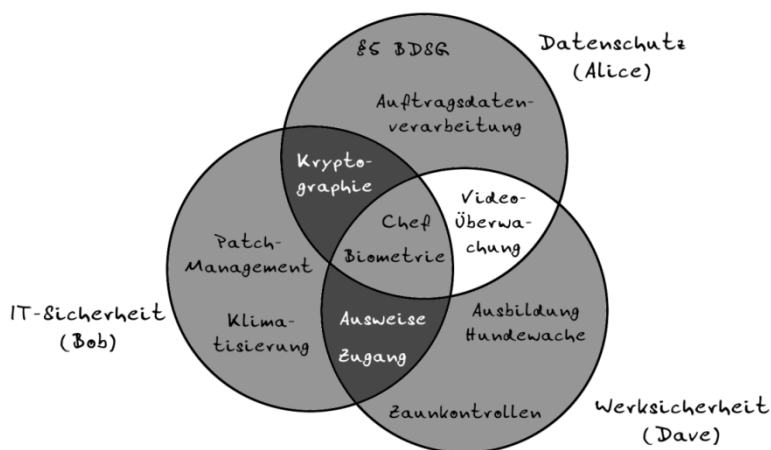
#### 1.2.4.1 Fallbeispiel: Das Pharma-Unternehmen ExAmple AG

In der ExAmple AG<sup>23</sup> gibt es die Datenschutzbeauftragte Alice und den IT-Sicherheitsbeauftragten Bob. Dave sorgt für die Sicherheit des Werksgeländes. Die drei können ganz gut miteinander arbeiten. Für das nächste Jahr haben sie sich gewisse Themen als Schwerpunkte herausgesucht.

---

<sup>23</sup> example.com gemäß RFC 2606 Absatz 3. Reserved Example Second Level Domain Names: <http://www.rfc-editor.org/rfc/rfc2606.txt>

- ❖ Alice möchte §5 BDSG endlich richtig umsetzen, die Verträge zur Auftragsdatenverarbeitung an die aktuelle Gesetzeslage anpassen und verstärkt Verschlüsselung nutzen. Außerdem hat sie von Daves Plänen gehört, auf dem gesamten Werksgelände Videoüberwachung und biometrische Zugangskontrollen einzuführen. Das möchte sie wegen der damit verbundenen Datenschutzschwierigkeiten besser verhindern, auf jeden Fall aber aufschieben. Sie wünscht sich in Datenschutzfragen mehr Unterstützung vom Vorstand.
- ❖ Der IT-Sicherheitsbeauftragte Bob will das Patch-Management verbessern und die alte Klimatisierung der Serverräume modernisieren. Mit einer neuen Verschlüsselungssoftware will er neuen Angriffsvarianten begegnen. Er möchte den Zugang zu den Betriebsräumen sicherer gestalten und würde gerne andere Ausweise dazu einsetzen. Die Ausweise sollen aber keine biometrischen Merkmale enthalten. Bob fürchtet, dass die datenschutzrechtlichen Anforderungen an die technische Absicherung zu hoch werden könnten. Was ihn schon lange stört, ist das Desinteresse des Vorstands, wenn es um Sicherheit geht. In einem Telefonat hat der Vorstand ihm vorgeworfen, er sei der größte Arbeitsverhinderer der Firma.
- ❖ Dave hat die Nase voll davon, dass seit einiger Zeit immer wieder Medikamente aus den Lagern gestohlen werden. Er möchte die Ausbildung der Hundewache unter die Lupe nehmen, die Zaunkontrollen verstärken und das Werksgelände mit Videokameras überwachen. Der Zugang zu besonders gefährdeten Räumen soll mit neuen, biometrischen Ausweisen gesichert werden. Ihn stört, dass der Vorstand sich für die Vorfälle bisher nicht interessiert.



**Abbildung 1-13:** Kartoffeldiagramm der Sicherheit – Beispiel für konkrete Ziele der drei Sicherheitsexperten der ExAmple AG für das nächste Jahr

In Abbildung 1-13 sind die Ziele von Alice, Bob und Dave eingezeichnet. Im Kartoffeldiagramm wird deutlich, wo die drei an einem Strang ziehen und wo sie sich gegenseitig behindern. Wenn Sie sich an einen Tisch setzen und ihre Ziele miteinander koordinieren, kommen sie bestimmt weiter; wenn Sie es nicht tun, gefährden sie das einzige gemeinsame Ziel. Wenn sie mit ihren Entscheidungsvorlagen und Zielen gegeneinander arbeiten, werden Sie vor dem Vorstand weiterhin als Arbeitsverhinderer dastehen. Und das, obwohl sie nur um zwei Punkte streiten.<sup>24</sup>

Alice, Bob und Dave müssen nun auch ihre Zwänge, die Prioritäten und Risiken analysieren, um zu klären, nach welcher Musik auf der Security-Bühne getanzt werden soll. Eines steht fest: Wenn jeder eine andere Musik abspielt, finden die Akteure nie in den Takt.

Damit ist die Arbeit jedoch noch nicht erledigt. Wenn die Problemfelder der Sicherheitsexperten synchronisiert sind, müssen sie mit den Problemfeldern der anderen Akteure verglichen werden. Auch das lässt sich mit einem *Kartoffeldiagramm der Sicherheit* visualisieren. Zum Schluss dieses mehrstufigen Vorgehens liegen – wie versprochen – die Zwänge, Ziele, Prioritäten und Risiken wie eine übersichtliche Landkarte vor uns. Bevor es jedoch so weit ist müssen wir uns – nach den Chefs und den Experten – nun den eigentlich Betroffenen zuwenden.

### 1.3 Mitarbeiter

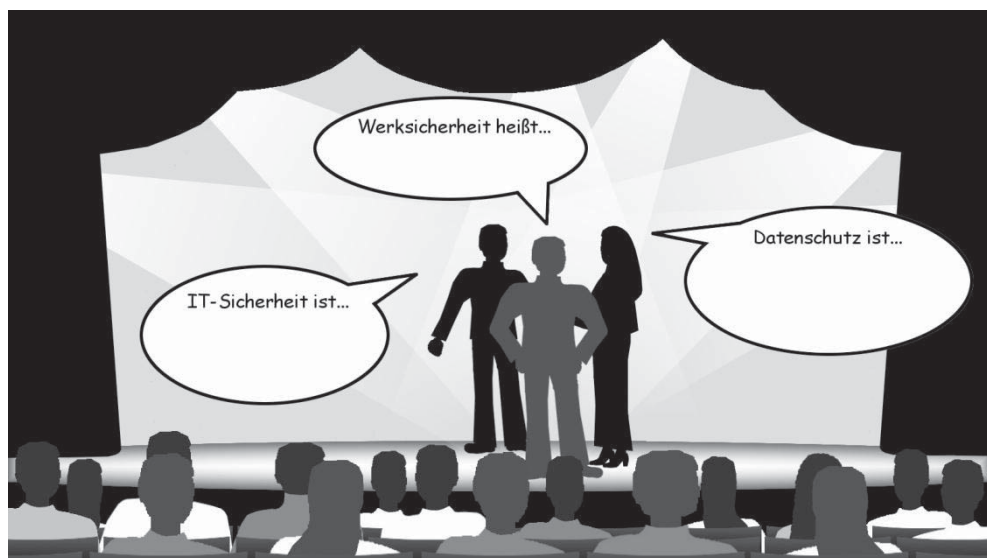
Die Mitarbeiter werden auf der Security-Bühne gerne vernachlässigt. In den meisten Fällen spielen sie ja nicht einmal mit, sondern sitzen im Publikum, verhalten sich ruhig und verursachen keine Probleme. Sie hören den Sicherheitsexperten aufmerksam zu – scheinbar. Wenn man herausfinden will, was die Mitarbeiter zu sagen haben, muss man sie alleine lassen. Aber Achtung: Die Security-Bühne spielt zwar immer vor ausverkauftem Haus, das Programm kommt aber selten gut an.

Kein Zweifel, dass zwischen den Sicherheitsexperten und den Mitarbeitern ein großes Missverständnis besteht. Spricht man mit einzelnen Kolleginnen oder Kollegen, sind sie einsichtig und verstehen, worum es den Sicherheitsexperten geht. Klar, sind die Argumente doch auf deren Seite. Mit ein bisschen Berufserfahrung zaubern diese immer einen Vorfall aus dem Ärmel, bei dem genau das passiert ist, was gerade als unmöglich bezeichnet wurde. Irgendwann

---

<sup>24</sup> Das gesamte Fallbeispiel finden Sie im OnlinePLUS-Service zu diesem Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

verlieren die Zuhörer dann die Lust. Es ist einfach ein zu einseitiges Gespräch, ein Kampf mit ungleichen Mitteln.



**Abbildung 1-14:** Alice, Bob und Dave sagen den Mitarbeitern, wo es lang geht



**Abbildung 1-15:** Hinter dem Rücken der Sicherheitsexperten

Viele Mitarbeiter denken sich: „Ich kann das Gesagte zwar nicht in meine Welt übertragen, weiß aber auch nicht, wie ich es widerlegen soll. Also Augen zu und durch.“ Verlassen die Experten dann die Security-Bühne, lässt man der Kritik dann freien

Lauf. Um zu verhindern, was in Abbildung 1-15 zu sehen ist, wollen wir diese Sache in einem Fallbeispiel nochmal genauer betrachten.

### 1.3.1 Fallbeispiel: Das Angebots-Fax

Dave, der Sicherheitsbeauftragte der ExAmple AG, geht über die Flure und kommt an einem der Bürogeräteräume vorbei, in dem Drucker, Scanner, Kopierer und auch ein Fax stehen.

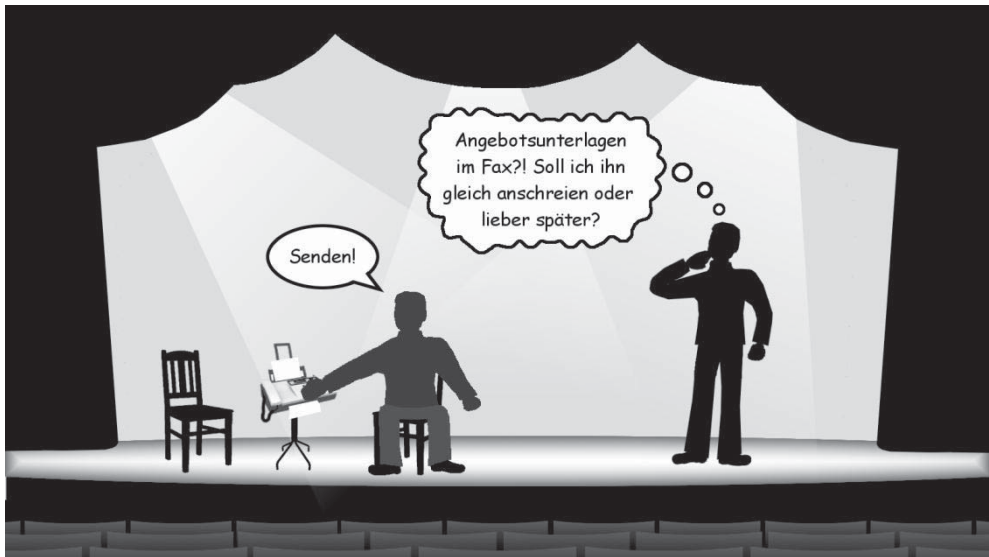


Abbildung 1-16: Konstruktiv geht anders!

Der Manager Ted steht am Fax und will eine vertrauliche Angebotsunterlage abschicken. Dave geht auf Ted zu und sagt:

*„Moment Mal, Sie können die Angebotsunterlage doch nicht per Fax an den Auftraggeber verschicken. Die müssen Sie einscannen und als verschlüsselte E-Mail verschicken.“*

*„Also bitte, dieses eine Fax wird uns schon nicht umbringen“, sagt Ted empört. „Bis ich das jetzt eingescannt, verschlüsselt und per E-Mail verschickt habe...! Keine Ahnung ob man denen überhaupt was verschlüsselt schicken kann. Außerdem wollen die ein Fax haben. Das dauert mir alles zu lang. Ich bin schließlich zum Arbeiten hier.“*

Dave erwidert routiniert: „Siemens hat durch ein einziges abgehörtes Fax schon einen Milliarden-Auftrag aus Südkorea für den ICE verloren<sup>25</sup>. Die hatten danach ganz viel Zeit zum Scannen und Verschlüsseln, weil sie den Auftrag verloren hatten.“

Was soll Ted da noch sagen? Das ICE-Beispiel ist *das* Totschlag-Argument am Faxgerät. Im Grunde verlässt Dave damit die sachliche Ebene. Man verlässt immer die sachliche Ebene, wenn man dem Gesprächspartner Argumente anbietet, die dieser weder richtig verstehen, noch widerlegen kann. Wer kann in so einer Situation schon mit den Begriffen Eintrittswahrscheinlichkeit und Annual Loss Expectancy<sup>26</sup> kontern? Abgesehen davon geht Daves Antwort gar nicht auf die Probleme ein, die der Mitarbeiter geschildert hat. Dave muss für die Sicherheit dieses Faxes bereit sein, das zu tun, was er von Ted erwartet: Zeit investieren. Spulen wir das Beispiel also nochmal kurz zurück:

(...) „Keine Ahnung ob man denen überhaupt was verschlüsselt schicken kann. Außerdem wollen die ein Fax haben. Das dauert mir alles zu lang. Ich bin schließlich zum Arbeiten hier“, hatte Ted gesagt.

Dave erwidert diesmal aber: „Kein Problem, ich helfe Ihnen dabei. Das Einscannen können wir gleich hier erledigen. Sie haben das Dokument 2 Minuten später als pdf in Ihrem Mail-Eingang. Dann rufen wir gemeinsam beim Sicherheitsbeauftragten des Auftraggebers an. Der wird uns sagen, wie wir verschlüsselt mit ihm kommunizieren können. In 15 Minuten ist die Sache erledigt und das Angebot raus. Dass wir so professionell vorgehen, kommt sicher gut an – da bin ich überzeugt.“

„15 Minuten? Da bin ich ja mal gespannt.“ Mit einem Blick auf die Uhr beginnt die Zeit für Dave zu laufen.

Das klingt viel besser. Wenn Dave selbst an das ICE-Argument glaubt, dann muss er bereit sein, diese Zeit zu investieren, geht es bei diesem Fax doch um einen möglichen Schaden, der in etwa dem erwarteten Auftragsgewinn entspricht.

Dieses Beispiel hilft uns zu verstehen, wie sich die Security-Bühne für Mitarbeiter darstellt: Die Mitarbeiter sitzen einfach als laienhafte Zuschauer im Publikum.

---

<sup>25</sup> Siemens verlor 1993 einen milliarden schweren Auftrag zur Lieferung des ICE nach Südkorea. Der französische Geheimdienst DGSE soll Informationen aus einem abgehörten Fax an den Siemens-Konkurrenten weitergegeben haben, der daraufhin den Zuschlag bekam, z.B.: <http://www.spiegel.de/spiegel/print/d-16161215.html>; eingesehen am 09.09.2009

<sup>26</sup> Annual Loss Expectancy: je nach Autor definiert durch  
 ALE = Schadenshöhe – Schadenseinsparung + Security Invest oder  
 ALE = Schadenshöhe · Eintrittswahrscheinlichkeit

Mancher kennt sich vielleicht ein wenig besser aus als der Andere – die Masse konsumiert jedoch nur. Die Security-Bühne tritt für viele nur ein Mal im Jahr durch eine Informationsveranstaltung in Erscheinung. Mit denselben Problemen, wie im echten Theater: Einige sind müde und schlafen, Einige kommen zu spät und Andere gehen in der Pause und kommen nicht wieder.

Was hat der Sicherheitsbeauftragte also im zweiten Dialog besser gemacht? Um diese Frage zu beantworten, müssen wir uns daran erinnern, was wir zu Beginn dieses Kapitels gesagt haben: Alle Beteiligten haben ihre ganz eigenen Bühnen, auf denen sie alle irgendeine Hauptrolle spielen.

- ❖ Im ersten Dialog hat der Sicherheitsbeauftragte Dave sich einen Mitarbeiter gegriffen, ihn auf die Bühne gezerrt, ihn dort zur Rede gestellt und in ein Fachgespräch über Eintrittswahrscheinlichkeiten und Risiken verwickelt. Klar, dass Ted an dem Gespräch nicht sehr geistreich teilnehmen konnte.
- ❖ Im zweiten Dialog ist Dave hingegen von der Security-Bühne gestiegen und mit Ted gemeinsam zu dessen Bühne gegangen: Teds Bühne heißt Akquise-Bühne. Dort spielt Ted eine der Hauptrollen. Die Akquise-Bühne ist ziemlich wichtig für das Unternehmen und der Etat der Security-Bühne wird zum großen Teil aus deren Einnahmen bestritten. Das ist so eine Art Kultur-Förderprogramm und die Kultur, die damit gefördert wird heißt – Sie ahnen es schon – Sicherheitskultur.

Manchmal kommen die Regisseure und Helden der Security-Bühne nicht umhin: Sie müssen den Bühnen, auf denen ihre Fördergelder erwirtschaftet werden, einen Besuch abstatten. Viel zu selten werden diese Ausflüge unternommen. Viel zu selten wird das Programm der Security-Bühne dahingehend überprüft, ob es mit den anderen Bühnen harmoniert, oder ob es da eine Kluft gibt, die sich spätestens beim nächsten Vorfall offenbart.



Wo werden die Blockbuster des Unternehmens gespielt? Das ist eine wichtige Frage, die in der Sprache des BSI IT-Grundschutzes so lautet: Was sind die geschäftskritischen Prozesse? Diese Frage muss für jeden Geschäftsprozess und jede Fachaufgabe erörtert werden<sup>27</sup>. Dazu reicht es nicht aus, nur in Dokumentationen zu blättern. Selbst die diszipliniertesten Mitarbeiter kommen in Situationen, in denen sie von dem einst modellierten Prozessverlauf abweichen

---

<sup>27</sup> Bundesamt für Sicherheit in der Informationstechnik; BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise; 2008; Seite 18 u.a. 

und improvisieren müssen. Dafür sind sie ja eigentlich da: Sie sollen ja auf besondere Bedingungen reagieren und den Plan an die Realität anpassen. Wäre das nicht gewollt, könnte man auch einen Roboter die Arbeit machen lassen.

Während jedoch bei der Modellierung der Geschäftsprozesse die Sicherheitsexperten mitgearbeitet haben stehen die Mitarbeiter in der Realität alleine da. In Entscheidungssituationen sind sie auf den Wissensschatz angewiesen, den sie haben. Auch wenn es banal sein mag: Marketingexperten kennen sich mit Marketing aus, Vertriebler mit Vertrieb und Einkäufer mit Einkauf. Also beurteilen sie diese Situationen auch aus ihrer entsprechenden Perspektive.

In vielen Fällen wird aus der einmaligen Improvisation ein dauerhaftes Provisorium. Es ist also die eine Sache, anhand definierter Geschäftsprozesse Sicherheitsrichtlinien festzulegen, und eine andere, den Mitarbeitern Handlungssicherheit zu geben, wenn von diesen Richtlinien abgewichen werden muss. Oft genug hilft nur, vor Ort zu sein und den Akteuren aktiv unter die Arme zu greifen, wie im Beispiel gezeigt.

Man könnte jetzt die Frage stellen, warum Mitarbeiter nicht um Hilfe bitten, wenn sie merken, dass geplante Sicherheitsrichtlinien sich nicht realisieren lassen. Diese Frage ist berechtigt. Wer sie aber stellt, sollte sich vor Augen führen, dass Mitarbeiter permanent gegen Sicherheitsregeln verstoßen. Dass sie nicht den ganzen Tag ein schlechtes Gewissen haben liegt einzig daran, dass sie gar nicht alle Sicherheitsmaßnahmen kennen. Die Fehler sind meist nicht allzu gravierend, und selbst den hoch motivierten Sicherheitsexperten – die ja eigentlich mit gutem Beispiel voran gehen – unterlaufen sie.

Machen Sie den Test und lesen Sie Ihr eigenes Sicherheitskonzept. Bei jeder Maßnahme fragen Sie sich, ob Sie in der letzten Woche dagegen verstoßen haben. Sie werden ziemlich oft feststellen, dass Sie von den Maßnahmen abgewichen sind:

- ❖ Sie haben sich sicher schon mal mit Angehörigen über einen Kollegen unterhalten, wo der wohnt, und ob er verheiratet ist und Kinder hat. Sind Sie sicher, dass Sie all diese Daten von ihm in der Kaffeepause erfahren haben? Oder waren die Informationen doch aus dem Personalbogen?
- ❖ Sie haben mit jemandem aus der Marketingabteilung über ein Projekt der Forschungsabteilung gesprochen? Hätte der diese Informationen auch bekommen, wenn er direkt in der Forschung angerufen hätte?

Sie finden bestimmt ein ähnliches Beispiel. Sie als Sicherheitsexperte haben natürlich vorher abgewägt, ob diese kleinen Verstöße in Ordnung gehen. Und genau so machen es die Mitarbeiter auch. Nur stützen diese sich bei ihrer kleinen „drive-by“-Risikoanalyse auf das Fachwissen, dass sie haben: Im Marketing, als

Vertriebler oder Einkäufer. Während bei Ihrer Entscheidung jahrelange Berufserfahrung als Sicherheitsexperte zugrunde liegt. Die Trefferrate dieser „drive-by“-Risikoanalysen der Mitarbeiter ist niederschmetternd schlecht. In Abschnitt 3.4.3.3 „drive-by“-Risikoanalysen werden wir versuchen sie zu erhöhen.

Es reicht für die Konzeptionierung der Security-Bühne nicht aus, den Text der anderen Bühnen zu lesen. Sie müssen die Vorstellung besuchen und im Text mitlesen – nur so fällt Ihnen auf, wann die Akteure davon abweichen. Um rauszufinden, wie groß die Diskrepanzen sein können, empfehle ich folgendes: Lesen Sie Goethes Faust und besuchen Sie danach eine aktuelle Vorstellung<sup>28</sup>. Sie werden feststellen, dass mancher Regisseur nicht einen Stein auf dem anderen gelassen hat. So ähnlich agieren die Regisseure der anderen Bühnen des Unternehmens auch, wenn sie es für nötig halten. Sie werden das aber nur erfahren, wenn Sie sich vor Ort ein Bild machen. Nur so erhalten Sie einen Einblick in die Problemfelder, die dort im Fokus stehen.

Wenden wir uns also den Problemfeldern der Mitarbeiter zu. Das ist nicht einfach und es wird komplexer, je granularer man die Sache angeht. Die Ziele eines Mitarbeiters ergeben sich aus dem Arbeitsvertrag und werden beispielsweise in Zielvereinbarungsgesprächen festgelegt. Es wird Ihnen sicher schwer fallen, die Zielvereinbarungen der Mitarbeiter in die Hände zu bekommen. Da sprechen dann *Datenschutzbedenken* dagegen, oder ähnliches. Das wäre so ein Fall, bei dem der Datenschutz zu den Zielen des Managements passt und daher verteidigt wird. Fünf Minuten später werden dieselben Zielvereinbarungen von dem Vorgesetzten als Vorlage an einen alten Studienfreund geschickt, der für seine Mitarbeiter auch Zielvereinbarungen schreiben muss. Dann passt der Datenschutz nicht mehr zu den Zielen des Managers, der dem Freund noch einen Gefallen schuldet. Interessanter sind diese persönlichen Ziele, weil diese in keinem Firmenprozess berücksichtigt sind und dazu neigen, Sicherheitsvorfälle auszulösen.

Es hilft nicht, einem Mitarbeiter zu garantieren, dass Zeitverzögerungen in Sicherheitsfragen keine Rolle spielen, wenn dieser Mitarbeiter am Hochzeitstag mit seiner Frau zum Essen verabredet ist und diese ihm garantiert hat, sich scheiden zu lassen, wenn er noch ein Mal zu spät kommt. Die Ziele, die das Unternehmen gesteckt hat und die äußeren Zwänge die auf dem Mitarbeiter an diesem Tag lasten, wirken sich auf seine Prioritäten aus. Prioritäten sind gewichtete Ziele und die Gewichtung verschiebt sich in dieser Situation deutlich. Auch die Risiken die er wahrnimmt werden sich nicht mehr mit denen decken, die *planbare Mitarbeiter* üblicherweise erkennen. Wenn er an diesem Tag in Stress gerät, dann kommt er

---

<sup>28</sup> Versuchen Sie es mit den Pressestimmen zu einer aktuellen Aufführung, beispielsweise hier: [http://www.theaterluebeck.de/index.php?seid=469&St\\_ID=132](http://www.theaterluebeck.de/index.php?seid=469&St_ID=132); eingesehen am 09.09.2009; archiviert unter <http://www.webcitation.org/5jffGgu6ha>

vielleicht, entgegen der Sicherheitsvorschriften, auf die Idee ein vertrauliches Papier mit in die U-Bahn zu nehmen, um es dort auf dem Nachhauseweg zu lesen. In seine „drive-by“-Risikoanalyse fließt nicht ein, dass er das Papier in der U-Bahn vergessen könnte oder ähnliches. Auf seiner Liste der Risiken steht auf den ersten drei Positionen: Scheidung, Scheidung und nochmal Scheidung.

Entscheidend ist, welche Security-Policy gilt: Will man Vorfälle verhindern, oder gibt man sich mit einem Schuldigen zufrieden. Wer als Sicherheitsexperte Vorfälle verhindern will, kommt nicht umhin, sich mit den Problemfeldern der einzelnen Mitarbeiter auseinanderzusetzen, sich ihnen zumindest anzunähern. Für den Anfang reicht ein Gespür dafür, welche Abteilung unter Zeitdruck arbeitet und welche genügend Zeit für alle Sicherheitsanforderungen hat. Wenn Sie Vorfälle verhindern wollen, müssen Sie für die Mitarbeiter als Ansprechpartner greifbar sein und ein Vertrauensverhältnis aufbauen. Immerhin müssen die Mitarbeiter damit rechnen, in Schwierigkeiten zu geraten, wenn sie bei Ihnen ihr Fehlverhalten thematisieren. Das darf unter keinen Umständen geschehen. Diese Art von Kommunikationsgeschick fordert sogar der IT-Grundschutz von den IT-Sicherheitsbeauftragten: *„Mitarbeiter (müssen) davon überzeugt werden, dass ehrliche Antworten nicht zu Problemen für sie selbst führen.“*<sup>29</sup>



**Abbildung 1-17:** Vertrauen ist Alles, wenn Sie wissen wollen, wo der Schuh drückt

<sup>29</sup> Bundesamt für Sicherheit in der Informationstechnik; BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise; 2008; Seite 27 

## 1.4 Personal- und Interessenvertretungen

Kommen wir nun zur letzten Gruppe von Protagonisten auf der Security-Bühne. Viele betrachten Personal- und Interessenvertretungen als das heiße Eisen schlechthin. Aus meiner Sicht keine gute Basis für eine fruchtbare Zusammenarbeit und der eigentliche Ausgangspunkt vieler Konflikte. Allerdings – das muss man auch eingestehen – kommen solche Vorbehalte nicht von ungefähr. Sie beruhen auf schlechten Erfahrungen der Vergangenheit. Wollen wir mit so einer schlechten Erfahrung beginnen:

Der Betriebsratsvorsitzende hat den Chef zur Rede gestellt, warum durch den IT-Sicherheitsbeauftragten E-Mails der Mitarbeiter kontrolliert werden. Der IT-Sicherheitsbeauftragte wird zum Chef zitiert, und dort nach allen Regeln der Kunst zurechtgewiesen. Der Chef sagt, er könne sich im Moment keinen Ärger mit dem Betriebsrat erlauben, da sie in wichtigen Verhandlungen steckten. Der IT-Sicherheitsbeauftragte bekommt noch ein abfälliges *„Die Mail-Leserei hört auf! Dafür haben wir Sie hier nicht eingestellt!“* zugeworfen und das Gespräch ist beendet. Wie konnte das passieren? Der IT-Sicherheitsbeauftragte war gewarnt: *„Nimm dich bloß vor dem Betriebsrat in Acht“*, hatte man ihm gesagt und er war ihm vorsichtshalber lange aus dem Weg gegangen und jetzt das. Dass er gar keine Mails gelesen hat sondern der Server lediglich die Metadaten der Mails protokolliert, hatte den Chef schon gar nicht mehr interessiert.

Aus dem Weg gehen ist wohl nicht die beste Idee. Die meisten Interessenvertretungen haben das Recht informiert zu werden, nicht sich zu informieren. Klar, dass sie sauer reagieren, wenn sie von einer Sache zum ersten Mal auf dem Flur hören. Aus meiner Erfahrung ist es gerade für Sicherheitsexperten sehr hilfreich auf die Interessenvertretungen zuzugehen. Ein Personalrat sagte einmal zu mir, er wäre nicht dazu da, Mitarbeiter zu schützen, die gegen die Regeln verstoßen. Im Gegenteil: Bei Verstößen gegen sinnvolle und abgestimmte Regeln sei eine Reaktion der Vorgesetzten unerlässlich.

Nach diesem Gespräch wurde mir klar, wie wichtig es sein kann, wenn eine Mitarbeitervertretung einer Maßnahme zustimmt und diese für sinnvoll und im Interesse aller erachtet. Wer will eine solche Maßnahme noch in Frage stellen ohne sich Ärger einzuhandeln. Bei Sicherheitsmaßnahmen geht es ja nicht um Richtungsentscheidungen, über die man ausführlich diskutieren kann. In den meisten Fällen geht es um klare Ursache-Wirkung Zusammenhänge, die Schaden abwenden sollen. Wenn die Geschäfts- oder Behördenleitung eine Maßnahme ablehnt, können Sie mit der Interessenvertretung vielleicht weiterkommen. Eine Möglichkeit, die sich gerade für Datenschützer lohnen kann. Vertreten diese doch in nicht unerheblichem Maße Mitarbeiterrechte.

Aber auch in anderen Fällen: Die Risiken aus den Problemfeldern der Chefs sind andere, wie die der Mitarbeiter. Wenn ein Geschäftsführer bereit ist, Risiken zu tragen, die für einen Geschäftsbereich existenzgefährdend sein könnten, sehen das die Mitarbeiter dieses Geschäftsbereichs sicher etwas anders. Das Ziel eines Geschäftsführers ist es vielleicht den Gewinn zu steigern, weil das von den Gesellschaftern mit einem Bonus honoriert wird. Das Ziel der Mitarbeiter könnte es hingegen sein, einen sicheren Arbeitsplatz zu haben, um ein Haus abzubezahlen. Wenn das Pokern für den Chef nicht aufgeht, kann er den Vorfall ja immer noch den Sicherheitsleuten in die Schuhe schieben.

Wenn Sie in so einem Dilemma feststecken, kann Ihnen eine gute Zusammenarbeit mit den Interessenvertretungen ihres Unternehmens oder Ihrer Behörde das Leben retten und das Thema für Sie ins Spiel bringen. Sicherheitsexperten genießen im Allgemeinen keinen Kündigungsschutz – einige Interessenvertreter schon.

Je nach Größe Ihres Unternehmens oder Ihrer Behörde steigen Sie beim Thema Interessenvertretungen allerdings auch in die große Politik ein. Das birgt natürlich auch Risiken, die hier nicht verschwiegen werden sollen. Wenn sie es jedoch geschickt anstellen, können Sie von der Zusammenarbeit profitieren. Sie müssen sich hier also besondere Mühe geben, die Problemfelder zu analysieren.

Lassen Sie sich aber in keinem Fall von den Unkenrufen abschrecken und kontaktieren Sie die Ansprechpartner in Ihrem Unternehmen frühzeitig. Sie können dabei nichts verlieren: Wenn der Betriebsrat ihre neu geboren Idee für eine Videoüberwachung des Werkstors nicht gut findet, wird er sie nicht besser finden, wenn Sie sie bis ins Detail ausgeplant haben. Wenn Sie aber immer wieder mal mit dem Betriebsrat über neue Bedrohungen und mögliche Gegenmaßnahmen sprechen, werden Sie bald ein Gespür dafür bekommen, was geht und was nicht.

Laden Sie doch die Interessenvertreter des Unternehmens oder der Behörde für die Sie arbeiten zu einer kleinen Privatvorstellung der Security-Bühne ein und gewähren Sie einen Einblick in Ihre Arbeit. Erklären Sie, wie Sicherheitsmaßnahmen zustande kommen und warum sie sein müssen, auch wenn es manchmal lästig ist. Mit ein wenig Geschick gewinnen Sie auf diesem Weg einen starken Verbündeten.

## 1.5 Zusammenfassung

Welchen Zwängen unterliegen die Protagonisten? Welche Ziele verfolgen sie mit welchen Prioritäten? Welche Risiken beunruhigen sie? Das waren die Fragen mit denen wir uns im Kapitel *Willkommen auf der Security-Bühne* auseinandergesetzt haben. Von der Geschäftsführung über die Sicherheitsexperten zu den Mitarbeitern und deren Interessenvertretungen haben wir gesehen, dass jeder Akteur seine eigenen Problemfelder hat, die man sich als Sicherheitsexperte

zunutze machen kann. Dadurch wird es möglich, die eigenen Ziele in die Ziele der Anderen zu übersetzen.

Mit dem Kartoffeldiagramm der Sicherheit können Sie die Schnittmengen mit den anderen Sicherheitsexperten Ihres Bereichs identifizieren, um sich nicht gegenseitig auf den Füßen zu stehen. Die Problemfelder der Akteure der Security-Bühne sollten Sie in einer Tabelle gegenüberstellen und diese regelmäßig analysieren. Ein ausgearbeitetes Beispiel und Dokumentvorlagen für Ihre Analyse finden Sie im OnlinePLUS-Service zu diesem Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

Nachdem wir uns nun eingehend mit den Personen beschäftigt haben, mit denen man als Sicherheitsexperte zu tun hat, stehen im nächsten Kapitel die Besonderheiten im Mittelpunkt, die Security-Konflikte aufweisen. Warum kommt es überhaupt zu Konflikten? Liegt es an den Beteiligten, oder ist die Aufgabe, der sich Sicherheitsexperten Tag für Tag stellen müssen, einfach konfliktträchtig?

## 2 Arten von Security-Konflikten

*„Wasch mir den Pelz, aber mach mich nicht nass.“*

*Redensart*

Wenn ein Mitarbeiter seiner Arbeit nicht nachkommt, handelt er sich irgendwann Ärger ein; eine Konsequenz, die einigermaßen logisch erscheint. Die unlogische Umkehrung würde lauten, sich Ärger einzuhandeln, wenn man seine Arbeit ordnungsgemäß und gewissenhaft erledigt. Aber genau diese unlogische Umkehrung gilt für viele Sicherheitsexperten. Datenschützer, IT-Sicherheitsbeauftragte und Co. müssen damit leben, dass ihre Arbeit nicht immer gut ankommt, auch wenn sie gerade dafür eingestellt worden sind. Unter Umständen müssen sie mit Ärger rechnen, wenn sie zu sehr bohren. *„Keiner oder kaum ein IT Leiter oder Vorstand möchte, dass man in seinem System eine Sicherheitslücke findet. Selbst dann nicht, wenn er es sagt“*, schreibt ein Freelancer im IT-Security-Forum des Business-Netzwerks XING.<sup>30</sup>

Das ist eines der Grundprobleme, die Sicherheitsexperten in Konfliktsituationen bringen. Eine ausreichende Antwort auf die Frage, warum sie immer wieder in der Konflikt-Falle landen, ist es freilich nicht. Auf der Security-Bühne haben wir uns eingehend mit den Problemfeldern der Protagonisten befasst, mit ihren Zielen, Zwängen, Prioritäten und Risiken. Wir haben in Kapitel 1 den Rahmen gesteckt, in dem sich Security-Konflikte abspielen, ohne jedoch näher darauf einzugehen, ob es sich formal um Konflikte handelt, und nach welchen Gesetzmäßigkeiten sie entstehen. Wir werden daher unsere bisherigen Erfahrungen mit der Security-Bühne in den folgenden Abschnitten systematisieren. Am Ende des zweiten Kapitels ist dann das Handwerkszeug zusammen, um als Sicherheitsexperte Security-Konflikte verhindern zu können.

Wir werden uns in diesem Kapitel einige ausgewählte Modelle des Konfliktmanagements ansehen und anhand dieser die Eigenarten von Security-Konflikten erhellen. Ziel ist es, Klarheit über spezielle Kommunikationssituation zu erhalten, in denen Sicherheitsexperten Tag für Tag stecken. Die Modelle beleuchten das Thema jeweils aus einem ganz eigenen Winkel und sind – wie z.B. das Normenkreuz nach Gouthier (Abschnitt 2.3) – ursprünglich gar nicht für die Security-Branche entwickelt. Man merkt jedoch schnell, dass sie gute Arbeit

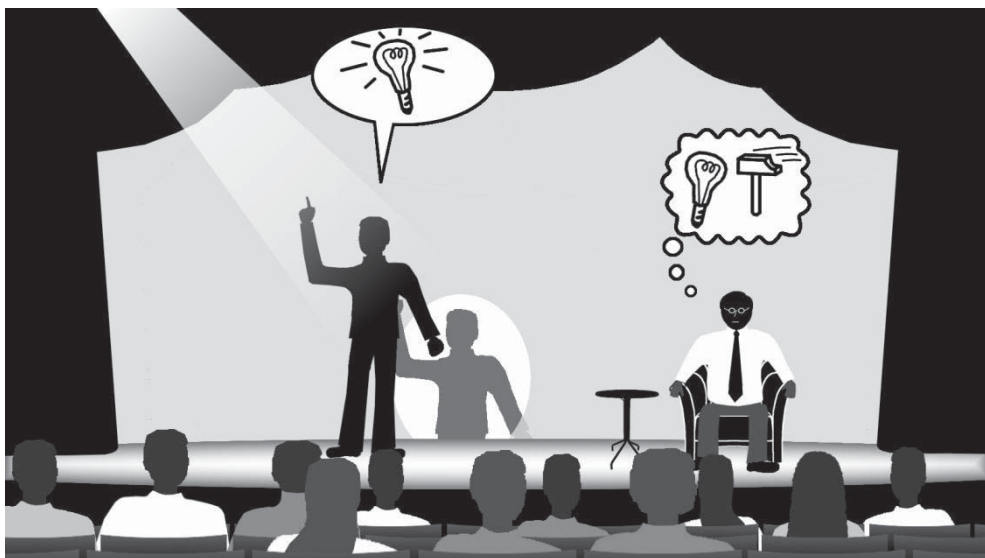
---

<sup>30</sup> <https://www.xing.com/app/forum?op=showarticles;id=7816814>; eingesehen am 14.09.2009; archiviert unter <http://www.webcitation.org/5jmSZadZX>

leisten, die Probleme zu verstehen, denen man sich als Datenschutz- oder IT-Sicherheitsbeauftragter stellen muss.

## 2.1 Was sind Security-Konflikte

Bevor wir zu den Modellen kommen, müssen wir uns fragen, was eigentlich Konflikte sind. Unzählige Bücher sind bereits über Konflikte geschrieben worden und man könnte meinen, dass diese Frage hinlänglich geklärt sei. Sind sie einfach eine Form des Streits? Was macht Konflikte aus? Ab wann kann man von einem Konflikt sprechen und wann ist man stattdessen zweierlei Meinung? Was im Rahmen dieses Buchs aber am meisten interessiert: Was im Speziellen sind Security-Konflikte? All diesen Fragen werden wir nun auf den Grund gehen.



**Abbildung 2-1:** Konfliktsituation: Ein Akteur beeinträchtigt die Interessen des anderen.<sup>31</sup>

Bevor man eine Meinungsverschiedenheit als Konflikt bezeichnet, müssen einige Voraussetzungen erfüllt sein. Auch wenn in der Literatur unterschiedliche Definitionen und Herangehensweisen anzutreffen sind, so lassen sich diese doch alle auf einen gemeinsamen Nenner bringen, der hier vorgestellt werden soll. Konflikte drehen sich immer um eine gewisse Anzahl voneinander abhängiger Personen, deren gegensätzliche Interessen, und den Willen diese durchzusetzen.

---

<sup>31</sup> Nach einer Zeichnung von Klaus Puth in: Regina Mahlmann; Konflikte managen: Psychologische Grundlagen, Modelle und Fallstudien; 2001; Beltz; ISBN 9783407363893; Seite 76

Die im Folgenden genannte Definition soll die Grundlage für die hier gemachten Überlegungen bilden.

Man spricht von einem Konflikt, wenn eine Interaktion zwischen mindestens zwei Akteuren die folgenden Merkmale aufweist<sup>32</sup>:

- ❖ Mindestens ein Akteur empfindet, vermutet oder erfährt eine Beeinträchtigung...
- ❖ ...bei der Verwirklichung seiner Interessen.
- ❖ Trotz einer empfundenen Abhängigkeit vom anderen Akteur...
- ❖ ...ist er bemüht, die Beeinträchtigung zu beseitigen bzw. seine Interessen durchzusetzen.

Im Zentrum von Konflikten stehen also die Interessen von Akteuren und die Art und Weise, wie sie sich bei deren Verwirklichung gegenseitig im Weg stehen. Diese Sichtweise auf einen Konflikt kommt unseren bisherigen Ergebnissen entgegen, haben wir diesen Zusammenhang doch schon bei den Problemfeldern unter den Stichworten *Ziele* und *Zwänge* näher betrachtet.

Eine gängige Forderung an Sicherheitssysteme ist es, dem Mensch die Entscheidung abzunehmen. Das System soll das Sicherheitsrisiko Mensch ausschalten. Während Unternehmensphilosophie, Führungsgrundsätze und andere Regelwerke den Betroffenen Handlungsspielräume ermöglichen, bleibt für Entscheidungen in den gängigen Security-Policies wenig Raum: Es ist alles verboten, was nicht ausdrücklich erlaubt ist und erlaubt wird nur, was abgesichert ist. Regeln bestimmen die Security-Szenerie.

Das ist ja an sich noch nicht problematisch, spielen Regeln doch insgesamt im Leben eine große Rolle. Wir alle sind Regeln mehr oder weniger gewohnt. Von Kindesbeinen an lernen wir uns in einer reglementierten Welt zurechtzufinden. Bis zu dem Tag, an dem wir unseren ersten Computer bekommen: Endlich frei! Windows fährt hoch und wir surfen mit Administrator-Rechten durch die unendlichen Weiten des Internet. Es wird installiert, was gefällt – Adware, Spyware und Trojaner inklusive. Auf dem Computer ist ja „*nichts drauf*“ und bei der üblichen Installationswut ist ohnehin alle drei Monate die Recovery-CD im Einsatz – dann ist alles wieder sauber. Wir melden uns fleißig bei Freemail-Anbietern, in Portalen und sozialen Netzwerken an und geben dabei so manches persönliche Detail bekannt – keiner hinterfragt wozu. Rund um den Monitor im privaten Arbeitszimmer kleben Passwortzettel, liegen PIN-Briefe und Zugangsdaten – my home ist my castle! So wie wir unseren privaten Computer

---

<sup>32</sup> Regina Mahlmann; Konflikte managen: Psychologische Grundlagen, Modelle und Fallstudien; 2001; Beltz; ISBN 9783407363893; Seite 18 

bedienen, so nutzen wir auch unser privates Handy, den WLAN-Router, die Telefonanlage: Selbstverwirklichung steht im Vordergrund.

In Sachen Security haben wir alle eine ziemlich antiautoritäre Erziehung hinter uns. Unter diesen Umständen sind Regeln schwer zu verkraften. Es wäre für Anwender dieser Prägung schon schlimm genug, wenn die Security-Policy gemeint wäre wie die Unternehmensphilosophie: Wichtig, wenn möglich. Aber nein, sie lautet: Es ist alles verboten, was nicht ausdrücklich erlaubt ist! Nach Jahren und Jahrzehnten antiautoritärer Prägung kommt irgendwann der Tag des ersten Kontakts mit einem Sicherheitsexperten: In der Einführungsveranstaltung für die neuen Kolleginnen und Kollegen erklärt der, wie sich das in Zukunft mit Administrator-Rechten, Software, Clean Desk, Datenschutz, Handy und Co. verhält.



**Abbildung 2-2:** Konfliktsituation: Die Vorstellungen der Mitarbeiter werden mit den Sicherheitsrichtlinien konfrontiert.

Wenn wir nun wissen wollen, ob auf Dauer gut gehen kann, was in diesem Moment der Wahrheit aufeinander prallt, brauchen wir nur unsere Konflikt-Definition zu Rate ziehen:

- ❖ Eine Interaktion zwischen mindestens zwei Akteuren:  
*In unserem Fall sind das die Arbeitnehmer und die Sicherheitsexperten.*
- ❖ Ein Akteur empfindet, vermutet oder erfährt eine Beeinträchtigung:  
*Das wären zweifelsohne die Arbeitnehmer, die mit den Sicherheitsrichtlinien konfrontiert werden.*

- ❖ Gegen die Verwirklichung seiner Interessen:  
*Dies sind die Interessen der Arbeitnehmer, die durch die Sicherheitsrichtlinien nicht verwirklicht werden können: Administrator-Rechte, private Software, Zettel mit Passwörtern auf dem Schreibtisch etc.*
- ❖ Empfundene Abhängigkeit vom anderen Akteur:  
*Die Abhängigkeit schließlich entsteht aus dem Arbeitsverhältnis heraus.*

Bis hier her sind während der Einführungsveranstaltung für die neuen Mitarbeiter fast alle Konflikt-Voraussetzungen erfüllt. Wenn sich jetzt einfach alle an die Regeln halten, würde es keinen Konflikt geben. Wir wissen, dass die Realität anders aussieht. Wäre es nicht so, würden Sie dieses Buch nicht in Händen halten. Kommen wir also zur letzten Konflikt-Voraussetzung:

- ❖ Die Beeinträchtigung soll beseitigt werden und die Interessen werden von den Beinträchtigten weiterverfolgt:  
*Durch Software, die sich nicht in die Registry einträgt wird das Administrator-Problem gelöst. U3-Sticks und Ceedo<sup>33</sup>. Passwortzettel werden unter der Tastatur oder in der obersten Schublade des Schreibtischs versteckt etc.*

Die beschriebene Situation scheint ausweglos, der Konflikt zwischen den Sicherheitsexperten und den anderen Akteuren unter diesen Umständen unausweichlich. Mit der weit verbreiteten Holzhammermethode steuert man unweigerlich auf eine Konfliktsituation zu, in der einiges zu Bruch gehen kann.

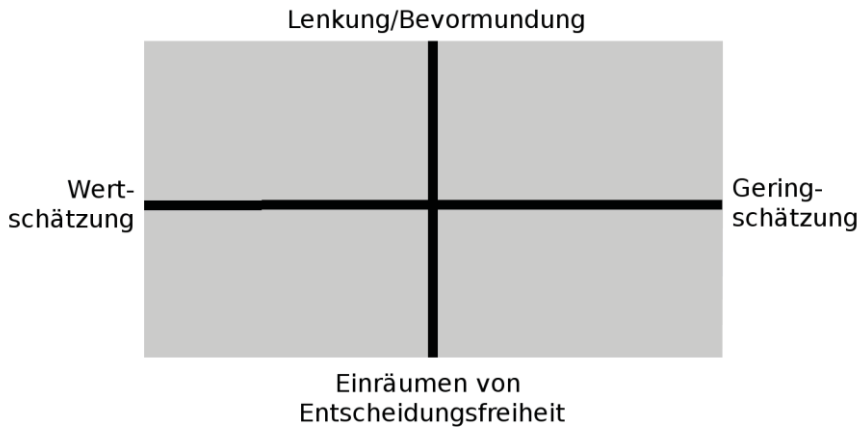
## 2.2 Verhaltenskreuz nach Schulz von Thun

Der letzte Abschnitt hat mehr Fragen aufgeworfen, als er Antworten gebracht hat. Wie konnte es so weit kommen und was ist daran falsch, mit dem risikoreichen und liederlichen Umgang mit der privaten IT-Ausstattung aufzuräumen? Daran ist nichts falsch, das ist ja das Dilemma, in dem sich Sicherheitsexperten befinden. Bevor ich Sie also gänzlich demotiviere, müssen wir beginnen nach einem Ausweg aus dieser Konflikt-Misere zu suchen. Zur Beschreibung von Konfliktsituationen schlägt Friedemann Schulz von Thun in seiner Reihe „Miteinander reden“ ein

---

<sup>33</sup> U3 und Ceedo sind Technologien, die auf externen Datenträgern eine Art Start-Menü zur Verfügung stellen, von dem aus man eigene Software auf beliebigen Computern ausführen kann, ohne Administrator-Privilegien besitzen zu müssen.

Verhaltenskreuz<sup>34</sup> vor, das uns bei der Suche nach einer Richtung als Landkarte dienen soll. Unser erster Schritt dabei ist, unseren Standort zu bestimmen.



**Abbildung 2-3:** Verhaltenskreuz nach Schulz von Thun

Schauen wir uns das Modell näher an: In zwei Dimensionen werden auf dem Verhaltenskreuz zuerst Wertschätzung und Geringschätzung und als Zweites Lenkung/Bevormundung und das Einräumen von Entscheidungsfreiheit aufgespannt. Das Verhaltenskreuz spricht mit diesen Dimensionen vor allem die Beziehungsseite der Kommunikation an.

### **Wertschätzung und Geringschätzung**

Zu einer wertschätzenden Kommunikation gehören Höflichkeit und Takt und freundliche Ermutigung. Ebenso wird eine Umkehrbarkeit des Sprachverhaltens gefordert: *„Was du nicht willst, das man dir tu, das füg' auch keinem andren zu!“* Mit Wertschätzung ist freilich nicht gemeint, sich gegenseitig Honig um den Mund zu schmieren oder die Worte in Watte zu packen.

Eine geringschätzende Kommunikation hingegen ist emotional kalt, abweisend und von oben herab. Man zeigt dem Gegenüber auf diese Weise seine Abneigung oder möchte ihn oder sie sogar lächerlich machen.

<sup>34</sup> Friedemann Schulz von Thun; Miteinander reden 1 - Störungen und Klärungen. Allgemeine Psychologie der Kommunikation; 1981; Rowohlt Taschenbuch Verlag; ISBN: 3499174898; Seite 162 ff

## Lenkung/Bevormundung und Einräumen von Entscheidungsfreiheit

Durch Lenkung oder Bevormundung versucht man den Kommunikationspartner weitgehend unter den eigenen Einfluss zu bringen. Die Sprache ist durch Anweisungen, Vorschriften und Verbote bestimmt. Zu viel Lenkung und Bevormundung löst inneren Widerstand aus. Das Einräumen von Entscheidungsfreiheit verzichtet hingegen auf solche Sprachmittel.

Security-Kommunikation, wie wir sie bisher kennen gelernt haben, spielt sich in den oberen beiden Quadranten des Verhaltenskreuzes von Seite 44 ab. Sicherheitssysteme sollen Entscheidungsspielräume ja bewusst einschränken und die Nutzer gezielt auf Kurs bringen. Meist ist die Situation zusätzlich so, dass der Security-Fachmann mit seinem Wissensvorsprung nicht verhindern kann, zusätzlich in den rechten Teil der Graphik abzudriften. Manch einer geht derart blauäugig und ablehnend an das Thema Security heran, dass es schwer fällt, dem mit Wertschätzung gegenüberzutreten: Konflikt vorprogrammiert!

### 2.2.1 Fallbeispiel: Das Angebots-Fax

Einzelne Äußerungen lassen sich in der emotionalen, sowie der Lenkungsdimension im Verhaltenskreuz einschätzen. Als Beispiel greifen wir auf die Situation aus dem Fallbeispiel von Seite 30 zurück. Der Sicherheitsbeauftragte Dave „erwischt“ den Manager Ted, wie der am Fax steht und eine vertrauliche Angebotsunterlage abschicken will. Natürlich kann er Ted direkt und ohne Umschweife auf seinen Fehler Aufmerksam machen:

*„Ich glaub‘ ich spinne! Hände weg von dem Fax! Vergessen, was im Sicherheitskonzept steht? Wer lesen kann ist klar im Vorteil!“*

Klar, dass Ted bei diesem bevormundenden und wenig wertschätzenden Angriff auf Gegenangriff schaltet. Ebenso wenig gut wäre es, wenn Dave resigniert:

*„Sie schon wieder. Klar: Angebotsunterlagen im Fax verschicken! Aber Sie machen ja sowieso was Sie wollen.“*

Die zwei bisher vorgestellten Arten Ted anzusprechen werden nicht zum Ziel führen, sondern eher das Gegenteil bewirken. Dave muss sich auf seinen Gesprächspartner einstellen, auch wenn es schwer fällt: Wertschätzung muss sein:

*„Hi Ted, schön Sie zu sehen. Wie geht’s? Angebotsunterlagen im Fax sind verboten. Sie müssen die Unterlagen anders übermitteln.“*

Das ist schon deutlich besser, weil es Teds Persönlichkeit nicht angreift und klar macht, was erlaubt ist und was nicht. Auf der anderen Seite wird Ted immer noch bevormundet. Das löst bei einigen Menschen Ablehnung aus, die man vermeiden kann, wenn man dafür sorgt, dass das Gespräch weiter gehen kann und Teds Ziele berücksichtigt werden:

*„Hi Ted, schön Sie zu sehen. Ich fürchte, dass Angebotsunterlagen im Fax verboten sind. Ist es wirklich so eilig?“*

Dave hat gesagt wo sein Problem liegt und Ted kann nun seine Meinung zum Thema sagen. Danach liegt es natürlich an Dave, an der Problemlösung mitzuwirken. Diese Bereitschaft muss natürlich vorausgesetzt werden. Die möglichen Antworten Daves sind in den jeweils passenden Quadranten des Verhaltenskreuzes eingetragen:



**Abbildung 2-4:** Die vier Antwortmöglichkeiten von Dave

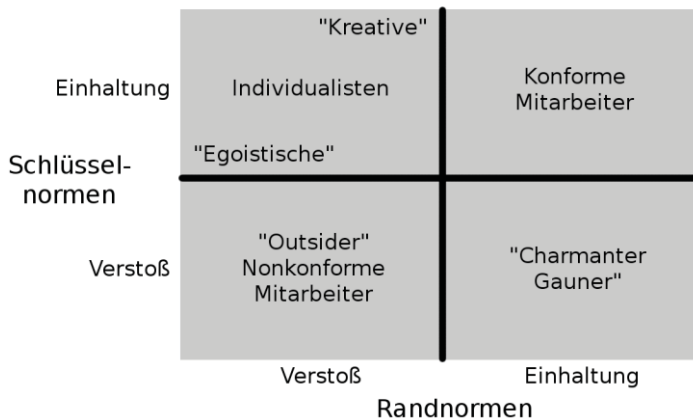
Das Verhaltenskreuz bildet also vier Quadranten, in denen man nun schauen muss, wo man steht. Will man Konflikte vermeiden und setzt auf nachhaltige Verhaltensänderungen kommt man nicht umhin, sich im Verhaltenskreuz nach unten links zu orientieren. Bevor wir jedoch in diese zweifelsohne lohnenswerte Richtung aufbrechen, sollten wir uns überlegen, wer dort auf uns wartet.

## 2.3 Normenkreuz nach Gouthier

Der Kunde ist König heißt der Grundsatz jeder Dienstleistung. Und wer König ist wird wertschätzend behandelt und hat allerlei Entscheidungsfreiheit. Mit diesen beiden Attributen schlagen wir im Verhaltenskreuz die richtige Richtung ein, um

Konflikten vorzubeugen. Aber auch Kunden unterliegen Regeln. Sicherheitsexperten müssen sich auf eine große Anzahl von Kunden einstellen und es lohnt sich, diese genauer zu betrachten und in Gruppen einzuteilen.

Matthias H. J. Gouthier<sup>35</sup> hat ursprünglich zur Beschreibung von Kundenbeziehungen ein Normenkreuz eingeführt, dass eine Einteilung in solche Kundengruppen ermöglicht. Es fokussiert auf das Kundenverhältnis im Dienstleistungsbereich und wird auch in der Konflikt-Literatur zitiert. Das liegt daran, dass die Frage im Mittelpunkt steht, inwieweit die Kunden sich an bestimmte Normen halten, die für die Beziehung zwischen Kunde und Dienstleister gelten. Es eignet sich hervorragend um das Verhältnis der Security-Profis mit ihren Kunden darzustellen.



**Abbildung 2-5:** Normenkreuz nach Gouthier

Die in einem Unternehmen oder einer Behörde vorgegebenen Security-Normen unterscheidet man im Normenkreuz nach den Schlüsselnormen (Muss- bzw. Grundnormen) und den Randnormen (Soll- bzw. Kann-Normen). Die Schlüsselnormen sind eine Grundvoraussetzung für die Aufrechterhaltung des Arbeitsvertrags. Hier werden Normen eingruppiert, welche die Legalität des Mitarbeiterverhaltens fordern. So führt es unweigerlich zur Kündigung, wenn man vertrauliche Entwicklungsdaten an die Konkurrenz weitergibt. Bei den Randnormen ist es zwar erwünscht, dass man sich an sie hält, ein Verstoß führt aber nicht unmittelbar zur Beendigung des Arbeitsverhältnisses. Hierzu gehört beispielsweise das Gebot, die Tür abzuschließen, auch wenn man das Büro nur

<sup>35</sup> Matthias H. J. Gouthier, Bernd Strauss; Kundenentwicklung im Dienstleistungsbereich; 2003; Gabler; ISBN 3824476754; Seite 48

kurz verlässt. Je nachdem, ob sich ein Mitarbeiter an die Normen hält oder nicht, kann man unterschiedliche Mitarbeitertypen identifizieren (siehe Abbildung 2-5).

Mitarbeiter, die sich sowohl an Schlüssel- als auch an Randnormen halten bezeichnet man als *konforme Mitarbeiter*. Für ein Unternehmen wären das etwa Mitarbeiter, die ihre Verschwiegenheitspflicht gemäß Datenschutzgesetz einhalten (Schlüsselnorm) und darüber hinaus regelmäßig an den internen Sicherheitsschulungen teilnehmen (Randnorm).

Mitarbeiter, die sich nicht an Schlüsselnormen halten, müssen aus dem System ausgeschlossen werden. Gouthier fordert das unabhängig davon, ob sie sich als *Outsider* entpuppen oder als *charmante Gauner*. Die Störung der Interaktion zwischen den Beteiligten – und damit das Konfliktpotential – ist in der unteren Hälfte des Normenkreuzes einfach zu groß. Es hilft nun mal nicht weiter, wenn der Mitarbeiter, der die vertraulichen Entwicklungsdaten an die Konkurrenz weitergegeben hat, immer seine Bürotür abschließt und sämtliche Sicherheitsschulungen aufmerksam verfolgt hat. Was in diesem Fall zählt, ist der Geheimnisverrat.

Bei den Mitarbeitern, die sich an Schlüsselnormen halten, sich aber bei den Randnormen nicht allzu gewissenhaft verhalten, sind die *kreativen Individualisten* für das Unternehmen oder die Behörde besonders wertvoll. Diese können den Sicherheitsexperten durch ihr abweichendes Verhalten Innovationspotential aufzeigen. Sie stellen damit quasi eine Qualitätssicherung der Randnormen sicher. Die *kreativen Individualisten* sind von den *egoistischen Individualisten* abzugrenzen, die sich einfach alles erlauben, was straffrei bleibt.

Wenn man Mitarbeiter nach diesem Schema gruppieren will, muss man sich zunächst im Klaren darüber sein, welche Sicherheitsmaßnahmen zu den Schlüsselnormen gehören und welche als Randnormen gelten sollen. Diese Frage ist aber nicht ganz so leicht zu beantworten, wie es scheint, sind doch die Randnormen nicht unmittelbar als solche zu erkennen. Die Unterscheidung ergibt sich eher aus der gelebten Praxis. Da ist es verständlich, dass Mitarbeiter schnell in die untere Hälfte des Normenkreuzes abrutschen. Viele Security-Konflikte entstehen in dieser Grauzone. Wer auf seinem Flur monatelang nur offene Türen sieht, ist zu Recht überrascht, wenn der Sicherheitsbeauftragte das plötzlich in den Bereich der Schlüsselnormen rücken will und eine Abmahnung verlangt.

Für die Sicherheitsexperten heißt das: Arbeit an der gelebten Praxis. Es ist nicht entscheidend, ob eine Norm im Sicherheitskonzept als Schlüsselnorm ausgewiesen wurde, oder ob sie objektiv eine sein sollte. Wichtig ist, dass bei Schlüsselnormen das eigene Fehlverhalten, vor dem Hintergrund der gelebten Praxis, überhaupt bemerkt werden kann.

Ein weiterer Aspekt, der den Security-Kunden von anderen Kunden unterscheidet ist der folgende: Normalerweise wird ein Kunde in irgendeiner Weise

Dienstleistungen nachfragen und ein Anbieter stellt sie ihm zur Verfügung. Die Security-Kundenbeziehung sieht aber meist so aus, dass die Verbote und Reglementierungen niemand nachfragt. Das Problem entsteht dadurch, dass sie trotzdem geliefert werden. Dadurch sinkt der Anteil *konformer Mitarbeiter*, wodurch wiederum die gelebte Praxis dahingehend beeinflusst wird, dass die sichtbare Grenze zwischen Schlüsselnormen und Randnormen zerfließt. Das macht es nahezu unmöglich, dass IT-Sicherheitsbeauftragte, Datenschützer und Co. in ihrem Kundenstamm *konforme Mitarbeiter* haben. Wenn der Schwerpunkt bei  *kreativen Individualisten* liegt ist schon viel gewonnen. Da diese mit ihrem Innovationspotential gut für die Weiterentwicklung eines Systems sind, bietet das Chancen, die Sicherheitskultur voran zu bringen.

Versuchen wir nun, die bisherigen Überlegungen zusammenzufassen: Das Verhaltenskreuz hat gezeigt, dass wir mit wertschätzendem Verhalten und mehr Entscheidungsfreiheit das Konfliktpotential reduzieren können. Im Normenkreuz sind besonders die  *kreativen Individualisten* von Interesse. Kombiniert man diese beiden Folgerungen, gelangt man zu einem Ansatz, mit dem man einiges erreichen kann.

| Verhaltenskreuz<br>Normenkreuz | wertschätzend/<br>entscheidungsfrei | wertschätzend/<br>lenkend | geringschätzend/<br>lenkend |
|--------------------------------|-------------------------------------|---------------------------|-----------------------------|
| Outsider                       |                                     |                           | X                           |
| Charmante Gauner               |                                     |                           | X                           |
| Egoistische Individualisten    |                                     | X-----X                   |                             |
| Konforme Mitarbeiter           |                                     | X                         |                             |
| Kreative Individualisten       | X-----X                             |                           |                             |

**Tabelle 2-1:** Kombination von Verhaltenskreuz und Normenkreuz

In Tabelle 2-1 wird die Kombination von Verhaltenskreuz und Normenkreuz übersichtlich dargestellt und vorgeschlagen, mit welchem Verhalten man welcher Mitarbeitergruppe begegnen sollte. Aus dem Verhaltenskreuz übernehmen wir jedoch nicht alle Verhaltenskombinationen, da dem Duo geringschätzend und entscheidungsfrei wenig Positives abgewonnen werden kann.

Arbeiten wir uns nun von oben nach unten durch die Tabelle: Während bei den  *Outsidern* und den  *charmanten Gaunern* außer Frage steht, auf weitere Entscheidungsspielräume zu verzichten und klar zu machen, dass das gezeigte Verhalten inakzeptabel ist, kann man den  *egoistischen Individualisten* schon mit mehr Verständnis begegnen. Immerhin halten sie sich an die wichtigen

Schlüsselnormen. Damit ist viel gewonnen. Das systematische auflehnen gegen jede Regel, die nicht gleich mit Kündigung bewährt ist, kann jedoch nicht geduldet werden. Auch hier sind Entscheidungsspielräume fehl am Platze.

Die Frage, ob es sinnvoll ist Entscheidungsspielräume einzuräumen, stellt sich zuerst bei den konformen Kunden – machen sie doch alles richtig. Spielräume bei Sicherheitsrichtlinien bergen jedoch Risiken, die nur eingegangen werden sollten, wenn damit ein Ziel verfolgt wird. *Konforme Mitarbeiter* verhalten sich aber richtig, auch ohne dass man noch einen zusätzlichen Anreiz setzen müsste. In diesem Fall gilt daher die alte Weisheit: Never change a running System! Erst wenn ein *konformer Mitarbeiter* sein Verhalten ändert, werden Maßnahmen erforderlich.

Mit den *kreativen Individualisten* schließlich müssen wir flexibel umgehen, wollen wir doch ihr Innovationspotential nutzen. Dass sie mit offenen Augen durch die Welt gehen und an den Sicherheitsrichtlinien mitarbeiten, kann durch ausgewählte Freiräume in eine Richtung gelenkt werden. Aber Vorsicht: Es *kann* nicht nur gelenkt werden, es *muss* gelenkt werden! Im Grunde gleicht dieses Vorgehen dem Spiel mit dem Feuer und darf nur unter strenger Aufsicht durchgeführt werden. Für den Augenblick reicht es jedoch, diese Möglichkeit im Hinterkopf zu behalten. Wir werden im weiteren Verlauf dieses Buchs darauf zurückkommen.



Die Kombination aus Verhaltens- und Normenkreuz bietet einige Ansatzpunkte, um den Scherbenhaufen aufzuräumen, den Abschnitt 2.1 hinterlassen hatte. Die Inhalte der folgenden Kapitel werden – neben den auf Seite 8 vorgestellten Problemfeldern – auch auf Tabelle 2-1 aufbauen. Damit ist ein wichtiger Meilenstein erreicht.

Wie geht es nun weiter? Im nächsten Abschnitt wird eine besondere Art von Security-Konflikt vorgestellt: Interessenkonflikte. Diese treffen vor allem Sicherheitsexperten, die ihre Arbeit nur nebenamtlich machen. Ein weiterer Aspekt der Interessenkonflikte ist die Frage „*Wer kontrolliert den Kontrolleur*“. Danach befasst sich Abschnitt 2.5 mit dem Paradoxon, dass erhöhte Sicherheitsmaßnahmen letztlich mit einem Vertrauensverlust verbunden sind. Den Abschluss des Kapitels bildet ein Fallbeispiel aus der ExAmple AG, die wir bereits kennengelernt haben.

## 2.4 Interessenkonflikte

Überall wo unterschiedliche Interessen aufeinanderprallen, kann man von Interessenkonflikten sprechen. Wir beschäftigen uns in diesem Sinne schon seit Beginn dieses Buchs mit Interessenkonflikten. Für diesen Abschnitt sind jedoch die

unterschiedlichen Interessen von Bedeutung, welche die Sicherheitsexperten mit sich selbst verhandeln müssen. Also nicht in einem offenen Gespräch zwischen zwei Parteien, sondern als unbeobachtetes Zwiegespräch vor dem Gericht des eigenen Gewissens.

Es gibt zwei Hauptgruppen von Interessenkonflikten: Eine, die sich eher im Unterbewussten abspielt und sich ohne böse Absicht negativ auf die Sicherheit auswirkt. Sie kann jeden treffen, der neben Sicherheit noch mit anderen Aufgaben betraut ist. Bei einer weiteren Gruppe von Interessenkonflikten, wird die Sicherheit bewusst und zur Erreichung eines anderen Ziels geschwächt. Für sie ist wenigstens unethisches Verhalten, unter Umständen ein gehöriges Maß an krimineller Energie ausschlaggebend.

### 2.4.1 Die „Zweit-Job-Falle“

Für Viele ist Security nur ein Nebenjob. Gerade in kleinen und mittleren Betrieben ist es üblich nebenamtliche IT-Sicherheitsbeauftragte und Datenschützer zu haben. Ein solches Vorgehen muss man nicht von vornherein verdammen. Warum sollte nicht der IT-Leiter gleichzeitig der IT-Sicherheitsbeauftragte sein oder jemand aus der Personalabteilung als Datenschutzbeauftragter bestellt werden? So übernimmt jemand die Kontrollfunktion, der sich nicht lange einarbeiten muss und etwas von der Materie versteht. Wenn die Personalressourcen knapp sind, spricht viel dafür, zwei Tätigkeiten in Personalunion wahrzunehmen.

Wer jedoch zwei Aufgaben gleichzeitig wahrnimmt, steht täglich vor der Entscheidung: Heute lieber die eine und morgen lieber die andere Aufgabe. Man muss bedenken, dass gerade beim Thema Security dieser Interessenkonflikt fast immer eine Entscheidung zwischen gemischtem Eis oder trockenem Brot ist. In den seltensten Fällen wird man von Montagmorgen bis Mittwochmittag Personalbearbeiter sein können, um sich dann den Rest der Woche dem Datenschutz zu widmen. Selbst wenn: Im zweiten Teil der Woche würde man regelmäßig mit Vorgängen aus der Personalbearbeitung gestört werden, weil das *„nun mal wichtiger ist und dringender bis nächste Woche fertig werden muss“*. Wenn der betroffene Personalbearbeiter jedoch Dienstag zu seinem Abteilungsleiter sagt, dass er am Verfahrensverzeichnis nach §4e BDSG arbeiten muss, dann *„hat das sicher auch noch bis Donnerstag Zeit“*.

Ein ähnlicher Fall beschäftigte bereits 1994 den Ersten Senat des Bundesarbeitsgerichts (BAG). Hier sollte eine EDV-Fachkraft zusätzlich Datenschutzbeauftragter werden. Der Betriebsrat hatte sich wegen des entstehenden Interessenkonflikts gegen die zusätzliche Tätigkeit gewandt. Im Leitsatz zum Gerichtsbeschluss heißt es: *„Bedenken gegen die Zuverlässigkeit können sich daraus ergeben, dass der Arbeitnehmer neben seiner Aufgabe als*

*Datenschutzbeauftragter Tätigkeiten ausübt, die mit seiner Kontrollfunktion unvereinbar sind, weil sie den Arbeitnehmer in einen Interessenkonflikt geraten lassen.“<sup>36</sup>*



**Abbildung 2-6:** Interessenkonflikt: Gemischtes Eis oder lieber trocken Brot

Werden Sicherheitspositionen also in Zweitfunktion besetzt, sind die sich widerstrebenden Interessen mehr als nur am Rande zu berücksichtigen. Eingangs haben wir uns mit der These beschäftigt, dass Datenschutzbeauftragte zwar bestellt werden, aber eigentlich niemand hören will, was sie zu sagen haben. In dem Fall, der 1994 das BAG beschäftigte fängt dieses Problem für den Datenschutzbeauftragten sehr früh an: Als der Chef die Bestellung unterschrieben hatte, hätte die erste Amtshandlung des Datenschutzbeauftragten sein müssen, die Bestellung in Frage zu stellen – zum Glück hatte das damals der Betriebsrat für den Datenschutzbeauftragten übernommen. Erinnern wir uns an dieser Stelle kurz an die in Abschnitt 1.4 gezeigten Chancen einer fruchtbaren Zusammenarbeit mit den Personal und Interessenvertretungen.

Nun wäre das Problem der inneren Zerrissenheit an sich schon schlimm genug, könnte man sie für sich behalten. Will man die Sicherheitsposition jedoch mit dem nötigen Ernst wahrnehmen, bleibt nichts anderes übrig als den Interessenkonflikt bei jeder Gelegenheit zu thematisieren. Hier kommen wir dem Kern des Problems schon sehr nahe. Was soll der Mitarbeiter im nächsten Small-Talk mit der Geschäftsleitung thematisieren? Irgendwelche Sicherheitsprobleme (trocken Brot)

<sup>36</sup> BAG; Beschluss des 1. Senats; Mitbestimmung des Betriebsrates bei Versetzung eines Datenschutzbeauftragten; 22.03.1994; Aktenzeichen: 1 ABR 51/93 

oder doch lieber das kürzlich erfolgreich abgeschlossene Projekt, mit dem man sich für eine bessere Stelle empfehlen kann (gemischte Eis – mit Kirschen). Eigentlich müsste er die Sicherheitsprobleme ansprechen, dulden Sicherheitsprobleme doch keinen Aufschub. Schnapp – die „Zweit-Job-Falle“ ist zu!

#### 2.4.2 Wer kontrolliert den Kontrolleur?

Bereits im Abschnitt über die Sicherheitsbeauftragten stand uns Pawero Pate, der Sicherheitschef aus dem Tal der Könige. Pawero musste zur Zeit des Pharaos Ramses IX (1127/1128 bis 1100 v. Chr.) einer Plage von Grabräubern Herr werden. Leider konnten sich die Plünderer zu dieser Zeit bei den Sicherheitsbeamten durch Bestechung mit der Beute freikaufen. An der Spitze derer, die die Hand aufhielten stand: Pawero selbst. Letztlich stolperte er über den Fall des Grabräubers Amenpanufer, der sich nicht freikaufen konnte und unter Folter auspackte. Bis es soweit war, ermöglichte es Paweros Position jedoch, die Ermittlungen zu seinen Gunsten zu beeinflussen und seine Beteiligung zu verschleiern.<sup>37</sup>

Wieder drängt sich die Frage auf, ob man Vorfälle verhindern will, oder ob man nur einen Schuldigen braucht. Wer ausschließen will, dass ein Sicherheitssystem rissig wird, muss die Frage stellen: Wer kontrolliert den Kontrolleur? Nun müssen die Risse nicht gleich so groß sein, wie bei Pawero. Als er durch Amenpanufer zu Fall gebracht wurde, war es freilich zu spät. Wahrscheinlich fing es aber mit mehr oder weniger kleinen Verfehlungen an. So weit müsste man zurückgreifen, wenn man die große Verfehlung am Ende verhindern wollte.

Was hält den IT-Sicherheitsbeauftragten ab, am Arbeitsplatz mehr privat zu surfen wie erlaubt, wenn er doch der einzige ist, der die Protokolldateien der Server einsehen kann? Was hindert den Sicherheitsbeauftragten daran, den Eintrag im eigenen polizeilichen Führungszeugnis zu verschweigen? Und wer sollte den Datenschutzbeauftragten aus der Personalabteilung dabei erwischen, die Leistungsbeurteilungen der Abteilungsleiter zu sammeln und mit nach Hause zu nehmen? Alle drei unterliegen der Versuchung, sich nicht selbst kontrollieren zu müssen.

Die Versuchung wächst, wenn die Sicherheitsfunktion nicht hauptamtlich wahrgenommen wird, sondern als Nebenjob, wie wir es im vorigen Abschnitt bereits erörtert haben. Insbesondere unterliegen die Betroffenen in dieser Situation in ihrer Haupttätigkeit denselben Zwängen, wie die normalen Mitarbeiter und schnell werden in der „drive-by“-Risikoanalyse auch dieselben Fehleinschätzungen getroffen.

---

<sup>37</sup> Pascal Vernus; *Affairs and Scandals in Ancient Egypt*; 2003; Cornell University Press; ISBN 978-0801440786; Seite 5 ff 

Um der Versuchung zu widerstehen, braucht es ein gehöriges Maß an persönlicher Integrität und Disziplin. Selbst Pawero wird sich nicht vorgenommen haben Sicherheitschef im Tal der Könige zu werden, nur weil er dort einen Grabräuberring hochziehen kann. Auch er wird sich dieser Rolle in kleinen Schritten angenähert haben. Diese kleinen Schritte entsprechen einem Spiel mit dem Feuer. Steht man weit genug von den Flammen entfernt, kann man sich ihnen ohne Gefahr einen Schritt nähern, danach noch einen Schritt. Von Schritt zu Schritt wird es wärmer, aber noch nicht heiß. Bis man sich verbrennt, oder gar in die Flammen gestoßen wird – wie Pawero von Amenpanufer.

Als Sicherheitsexperte ist man dieser Versuchung täglich ausgesetzt. Man sollte deshalb bei der Sicherheitskonzeption nicht nur an alle anderen Mitarbeiter im Unternehmen oder der Behörde denken. Man muss sich selbst in die Risikoanalyse mit einbeziehen, so wie der nebenamtliche Datenschutzbeauftragte aus der EDV-Abteilung, der seinen Arbeitgeber auf den Beschluss des Bundesarbeitsgerichts aufmerksam macht. Und auch der IT-Sicherheitsbeauftragte, der sein Administratorkonto nach dem Vier-Augen-Prinzip nur im Beisein eines weiteren Administrators benutzt und die Zugriffe dokumentiert, tut genau das.

Es gibt wohl nichts Verheerenderes für Sicherheitsexperten, als gegen die eigenen Sicherheitsrichtlinien zu verstoßen. Glaubwürdigkeit und Vertrauen gehen so dauerhaft verloren. Die Beschränkung der eigenen Möglichkeiten steigert hingegen das Vertrauen in den Kontrolleur.

Vertrauen spielt eine große Rolle bei der Vermeidung von Konflikten. In der Definition von Konflikten auf Seite 41 wird gefordert, dass ein Akteur eine Beeinträchtigt bei der Verwirklichung seiner Interessen empfindet, vermutet oder erfährt. Es muss also keine wirkliche Beeinträchtigung vorliegen, es reicht aus, dass eine Beeinträchtigung *empfunden* oder *vermutet* wird. Dem kann man nur mit vertrauensbildenden Maßnahmen entgegenwirken.

## 2.5 Vertrauensverlust durch Sicherheitsmaßnahmen

Die Überschrift dieses Abschnitts ist gleichzeitig eine These, die nicht unbedingt auf den ersten Blick einleuchtet. Wie wir gesehen haben, können Konflikte in einer vertrauensvollen Umgebung vermieden werden. Ein prüfender Blick lohnt sich, denn für Vertrauensverlust gilt: Je weniger man den Mitmenschen vertraut, desto eher vermutet man, dass die eigenen Interessen missachtet werden könnten und desto eher fühlt man sich beeinträchtigt.

Zunächst muss man klären, was Vertrauen ist. Durch was ist ein vertrauensvoller Umgang gekennzeichnet? Die Antwort fällt leichter, wenn man sie von der entgegengesetzten Seite angeht: Demnach ist Vertrauen vor allem ein Zustand, in dem keine gegensätzlichen Empfindungen, wie etwa Misstrauen, vorkommen. Der

zweite zentrale Begriff aus der Überschrift lautet Sicherheit. Sicherheit wird im Allgemeinen als ein Zustand beschrieben, der frei von Gefahr ist. Auch hier wird der Zustand durch die fehlenden Merkmale beschrieben. Vertrauen und Sicherheit sind bei dieser Sichtweise zum Einen das Fehlen von Misstrauen und zum Anderen das Fehlen von Gefahr.

Wie müsste eine Gemeinschaft sein, in der alle sicher sind? Nach den bisherigen Überlegungen dürfte in einer solchen Gemeinschaft von keinem Gefahr ausgehen. Wenn aber von keinem eine Gefahr ausginge, dann gäbe es auch keinen Grund, sich gegenseitig zu misstrauen. Man kann also sagen, dass in dieser Gemeinschaft alle sicher sind und gegenseitiges Vertrauen herrscht. Sicherheit und Vertrauen hängen also eng miteinander zusammen und stehen daher in einer Wechselbeziehung zueinander.

Was also passiert, wenn aus einer gefahrfreien Gemeinschaft einzelne ausscheren und zur Gefahr werden? Das würde bedeuten, dass es ab dann einen Grund gäbe, seinem Gegenüber zu misstrauen. Mit der verlorenen Sicherheit der Gemeinschaft wäre auch das Vertrauen untereinander verloren gegangen. Am ehesten merkt man diesen Verlust, wenn er abrupt geschieht, beispielsweise, wenn man von einer freundlichen und sicheren Wohngegend in eine angespannte und unsichere zieht.<sup>38</sup> Instinktiv sehnt man sich nach der freundlicheren Umgebung zurück.

Die bisher nur abstrakt angesprochene Gemeinschaft könnte jede Gemeinschaft sein: Die Gesellschaft in der wir leben, das Miteinander von Firmen und Kaufleuten, das Internet oder das Firmennetz. Egal wo, Menschen sehnen sich nach Vertrauen: Kaufleute wollen, dass der Vertrag mit Handschlag mehr Gewicht hat, als der Vertrag auf hundert Seiten Papier; Liebespaare wollen, dass das Treueversprechen vor dem Traualtar nicht durch einen viel genaueren und detaillierteren Ehevertrag verwässert wird; Urlauber vor dem Mietwagentresen wollen sich nicht in Vertragsklauseln verlieren sondern einfach nur hören, dass der Vermieter hunderttausende zufriedene Kunden hat, deren Vertrauen nicht enttäuscht wurde. Menschen wollen einander vertrauen, selbst dann, wenn sie genau wissen, dass sie mit sehr hoher Wahrscheinlichkeit enttäuscht werden, egal ob Geschäfts-, Ehe- oder Mietvertrag.

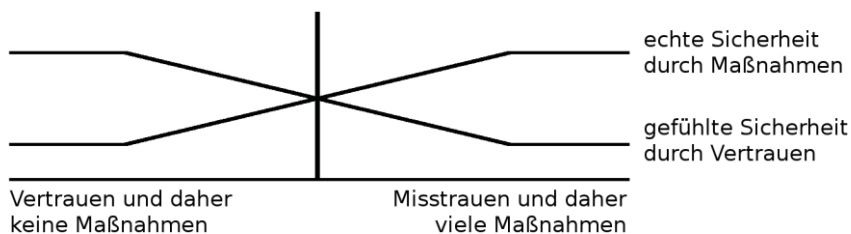
Was für eine Funktion haben Verträge? Im Kern sind es Sicherheitsmaßnahmen; Der Geschäftsvertrag schützt vor Missverständnissen zwischen den Kaufleuten; der Ehevertrag schützt das Vermögen der Eheleute im Streitfall und der Kfz-Mietvertrag schützt vor einem bösen Erwachen, wenn man aus dem Urlaub zurück ist. Menschen wissen aber zumindest unterbewusst: Sicherheitsmaßnahmen braucht man nur dort, wo Gefahr herrscht und Gefahr ist

---

<sup>38</sup> Martin Hartmann, Claus Offe (Hrsg.); Vertrauen. Die Grundlage des sozialen Zusammenhalts; 2001; Campus Fachbuch; ISBN 978-3593367354; Seite 86 ☞

nicht nur schlecht für die Sicherheit, sondern auch schlecht fürs gegenseitige Vertrauen. An dem Ehemann, der einen Ehevertrag wünscht, kann aus diesem Blickwinkel nicht alles in Ordnung sein: Entweder traut er seiner Frau nicht über den Weg, oder er traut sich selbst nicht und meint, sie müsse vor ihm geschützt werden.

Die Menschen die sich für oder gegen diese Sicherheitsmaßnahmen entscheiden müssen, belassen lieber alles beim Alten, bevor sie sich damit auseinandersetzen, dass die Umgebung in der sie sich bewegen, ihr Vertrauen in keiner Weise rechtfertigt. Das liegt zum einen an einem ungerechtfertigten Optimismus: „Bei uns ist das Risiko einer Scheidung gleich 0! Das unterscheidet uns von all den anderen Liebespaaren.“ Zum anderen an einer ausgeprägten Trägheit, die im Allgemeinen dazu führt, dass wir alles beim Alten belassen, selbst wenn es unseren eigenen Interessen widerspricht. Mit der Zugewinnngemeinschaft gibt es in Deutschland ja automatisch einen Ehevertrag und der Autovermieter hat den Vertrag schon hunderttausenden, zufriedenen Kunden vorgelegt. Warum soll man jetzt diese eine unverständliche Klausel zum Stichwort Schadensfall hinterfragen?<sup>39</sup>



**Abbildung 2-7:** Vertrauen und Sicherheit in Wechselwirkung

Wir können nun die Abbildung von Seite 18 etwas präzisieren: Die echte Sicherheit steigt, wenn wir mehr misstrauen und viele Sicherheitsmaßnahmen umsetzen. Die gefühlte Sicherheit nimmt jedoch ab, da sich Menschen in vertrauensvollen Umgebungen, in denen Sicherheitsmaßnahmen unnötig sind wohler fühlen. Vielfach handeln sie dabei irrational und versuchen den vertrauensvollen Zustand herzustellen, indem sie die Sicherheitsmaßnahme ablehnen und für überzogen erklären. Instinktiv wollen alle Mitarbeiter in allen Unternehmen oder Behörden, dass man ohne Angst die Bürotüren offen lassen kann, ohne dass etwas gestohlen wird: „Hier wird nichts geklaut“, heißt es solange, bis dann doch etwas verschwindet.

<sup>39</sup> Richard H. Thaler, Cass R. Sunstein; Nudge: Wie man kluge Entscheidungen anstößt; 2009; Econ; ISBN 978-3-430-20081-3; Seite 51 ff

Was bedeuten der aufgezeigte Zusammenhang und die Beispiele für Sicherheitsexperten? Zunächst müssen sie bekannt sein, um zu verstehen, warum so viele Sicherheitsmaßnahmen auf Ablehnung stoßen und Mitarbeiter eine ungeheuerliche Kreativität an den Tag legen können, sich neue Wege zu überlegen, bei denen der Aspekt des Vertrauens wieder die Oberhand gewinnt. Das bedeutet, dass der gefühlte Vertrauensverlust, der durch Sicherheitsmaßnahmen entsteht, kompensiert werden muss. Hierzu werden vor allem starke kommunikative Fähigkeiten benötigt. Ein Sicherheitskonzept beschreibt nach Abbildung 2-7 nur die Kurve der echten Sicherheit: Gefährdungskatalog, Risikoanalyse und Maßnahmen.

Was benötigt wird, ist ein Konzept, dass die Kurve der gefühlten Sicherheit flankiert, die mit jedem Schritt der Sicherheitskonzeption abnimmt. Wer also Schreckgespenster an die Wand malt, darf seine Zuhörer nicht mit der Angst allein lassen, in einer Welt voller Misstrauen zu leben. Bei der Sicherheitskonzeption muss also solchen Maßnahmen der Vorzug gegeben werden, welche von den Beteiligten nicht erfordern, sich gegenseitig zu misstrauen. Misstrauen muss eine Sache der Sicherheitsexperten bleiben. Immer wenn eine Maßnahme von einem Mitarbeiter fordert, dem Gegenüber zu misstrauen, muss man damit rechnen, dass sie umgangen oder nicht umgesetzt wird. Es erfordert eine viel zu große Disziplin, einem anderen in die Augen zu schauen und ihm auch bei der hundertsten Begegnung noch zu zeigen, dass man ihm nicht traut.

## 2.6 Fallbeispiel: Mehr Unterstützung vom Chef

In Kapitel 2 haben bisher theoretische Überlegungen überwogen: Definitionen, Koordinatensysteme und Kurvenverläufe haben dominiert. Dabei ging es vor allem darum zu zeigen, mit welcher Art von Konflikten Sicherheitsexperten besonders zu kämpfen haben, was diese also von all den anderen Problemen des Alltags unterscheidet. Zum Abschluss des Kapitels geht der Fokus wieder in die ExAmple AG zu den Sicherheitsexperten Alice (Datenschutz), Bob (IT-Sicherheitsbeauftragter) und Dave (Werkssicherheit).

In Abschnitt 1.2.4.1 sind die drei übereingekommen<sup>40</sup>, dass sie sich alle mehr Unterstützung vom Vorstand wünschen. Bob wurde in einem Telefonat vom Vorstand als der größte Arbeitsverhinderer der Firma beschimpft und Dave bemängelt, dass der Vorstand kaum Interesse an den Vorfällen der letzten Zeit zeigt. Jetzt sitzen sie wieder zusammen und überlegen, wie sie ihr Ziel erreichen können.

---

<sup>40</sup> Das gesamte Fallbeispiel finden Sie im OnlinePLUS-Service zu diesem Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

Alice liest vor: „Hier steht: Ein Konflikt ist eine Interaktion zwischen mindestens zwei Akteuren, wenn mindestens ein Akteur eine Beeinträchtigung bei der Verwirklichung seiner Interessen empfindet, vermutet oder erfährt. Trotz einer empfundenen Abhängigkeit vom anderen Akteur ist er bemüht, die Beeinträchtigung zu beseitigen bzw. seine Interessen durchzusetzen.“

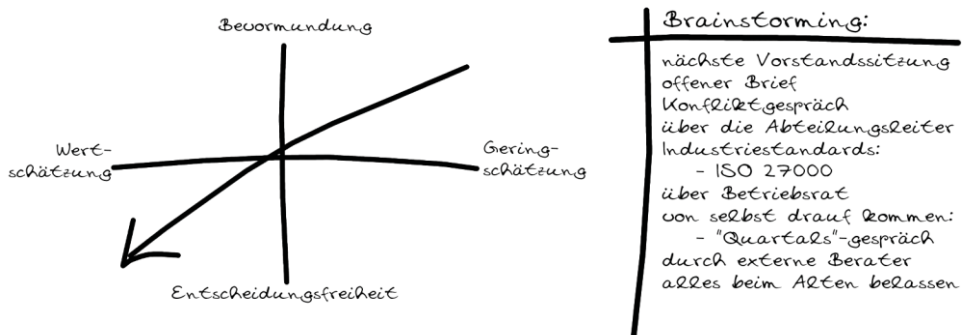
„Also abhängig ist der Chef ja wohl nicht von uns.“, unterbricht Dave.

„...aber wir von ihm, und wir sitzen ja wohl hier zusammen, um unsere Interessen durchzusetzen. Aber auch andersherum: Wenn der Chef uns nicht bräuchte, würde er uns ja wohl kündigen. Und beeinträchtigt fühlen wir uns ja offensichtlich alle.“

Alice steht auf und malt ein Kreuz ans Flipchart. Es ist das Verhaltenskreuz. Daneben kommt eine Tabelle mit der Überschrift Brainstorming:

„Welche Möglichkeiten haben wir, das Thema ‚mangelnde Unterstützung durch den Chef‘ anzusprechen?“ Sie malt durch das Normenkreuz einen Pfeil in Richtung des Quadranten Wertschätzung/ Entscheidungsfreiheit: „Da müssen wir hin!“

Alice, Bob und Dave sammeln einige Punkte in der Tabelle, die ihnen spontan einfallen. Alice ermahnt die beiden zwischendrin, dass Ziel Wertschätzung und Entscheidungsfreiheit nicht aus den Augen zu verlieren.



**Abbildung 2-8:** Alice, Bob und Dave analysieren ihre Situation

Nach ein paar Minuten haben sie ihre Ideen auf dem Flipchart zusammengeschrieben (Abbildung 2-8). Die Idee mit der nächsten Vorstandssitzung oder dem offenen Brief finden alle nicht so gut – der Pfeil zeigt nach unten links, nicht nach oben rechts. Eigentlich sind die Lösungen, die das Problem direkt ansprechen, alle nicht so gut geeignet, weil sie kaum Entscheidungsfreiheit lassen.

*„So, welche Alternative enthält am meisten Wertschätzung und Entscheidungsfreiheit?“, fragt Alice.*

*„Er muss von selbst drauf kommen“, antwortet Dave. „Wir müssen ihm die Sache so schildern, dass er von selbst drauf kommt, dass wir seine Unterstützung brauchen!“*

Bob ist von der Idee nicht so begeistert. Immerhin hat er vom Vorstand schon den Titel *größte Arbeitsverhinderer der Firma* bekommen. Eigentlich möchte er die Sache nicht weiter eskalieren lassen und sich zurückhalten. Mit seinem neuen Website-Projekt kann er beim Vorstand nun endlich mal Punkten. Diesen Erfolg will er eigentlich nicht gefährden und sich daher lieber voll auf das Website-Projekt konzentrieren. Bob sitzt in der „Zweit-Job-Falle“ fest. Auch wenn er sich mehr Unterstützung vom Chef wünscht, und gerne hätte, dass seine Arbeit als IT-Sicherheitsbeauftragter mehr gewürdigt würde: Im Moment ist das für ihn eine Entscheidung zwischen gemischtem Eis und trockenem Brot.

## 2.7 Zusammenfassung

Dieses Beispiel zeigt einerseits, wie leicht Sicherheitsexperten gute von schlechten Vorschlägen unterscheiden können, wenn sie Konflikte vermeiden wollen. Andererseits wird aber auch deutlich, in welchem Dilemma sie stecken, wenn es an deren Umsetzung geht. Aus diesen zwei Blickwinkeln beleuchtet Kapitel 2 die verschiedenen Arten von Security-Konflikten.

Den ersten Teil dieses Kapitels bilden die formale Definition eines Konflikts, das Verhaltenskreuz und das Normenkreuz. Diese liefern Instrumente, mit denen man Situationen oder Maßnahmen auf deren Konfliktpotential untersuchen kann. Im zweiten Teil wurden spezielle Herausforderungen vorgestellt, die auf Sicherheitsexperten zukommen: Interessenkonflikte und Vertrauensverlust durch Sicherheitsmaßnahmen.

Noch fehlen insbesondere die Mittel, mit denen man anstehende Sicherheitsmaßnahmen so vorbereitet, dass sie quasi von den Betroffenen selbst entschieden werden, so wie Dave im letzten Beispiel vorgeschlagen hatte. Schritt für Schritt nähern wir uns jedoch einem unserer Hauptziele: Der Vermeidung von Konflikten.

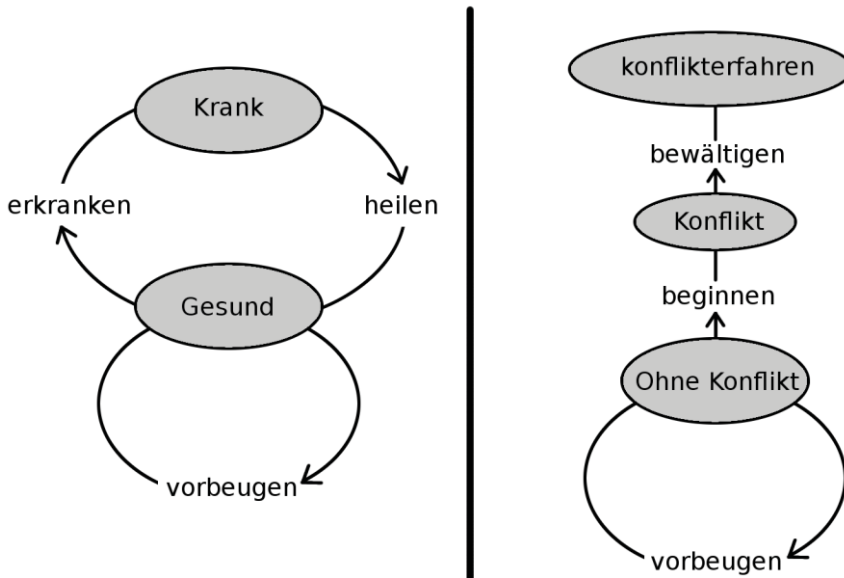


### 3 Konfliktprävention

*„Vorbeugen ist besser als Heilen.“*

*Hippokrates von Kos (ca. 460 bis 370 v. Chr)*

Heutzutage wird jeder präventiv tätig. Prävention ist ein beliebtes Modewort. Das rührt vor allem daher, dass es die Benennung eines klaren Ziels erspart. Man weiß zwar noch nicht ganz wohin, aber man weiß wohin nicht. Das Wort liefert quasi den gemeinsamen Feind, den kleinsten gemeinsamen Nenner, eben das, was vermieden werden soll. In der Medizin geht dieser Gedanke auf Hippokrates von Kos zurück. Aus seiner Formel „Vorbeugen ist besser als Heilen“ wird kurzerhand die Krankheitsprävention. Und bei der Konfliktprävention? Wie verhält es sich da? Wie würde Hippokrates' Formel übertragen auf Konflikte lauten? Vorbeugen ist besser als Bewältigen? Es stellt sich natürlich die Frage, ob es wirklich besser ist, Konflikte vorzubeugen, ihnen also aus dem Weg zu gehen, oder ob es besser ist, sie zu bewältigen. Wir wollen unter anderem dieser These im Folgenden auf den Grund gehen.



**Abbildung 3-1:** Vorbeugen statt Heilen

Wer das Wort Prävention benutzt stellt gleichzeitig eine These auf. Im Fall der Konfliktprävention lautet diese: Es gibt zwei Wege, die von einem Ausgangspunkt zu einem Ziel führen. Der eine Weg geht über einen Konflikt und dessen Bewältigung zum Ziel; der andere Weg geht ohne einen Konflikt mehr oder weniger direkt zu dem Ziel. In der Formel „*Vorbeugen ist besser als Heilen*“ sind Ausgangspunkt und Ziel gleich: Ein gesunder Mensch. Vorbeugen bedeutet also bereits am Ziel zu sein, und dort zu bleiben (vgl. Abbildung 3-1).

Ganz so einfach ist es aber auch bei den Krankheiten nicht: Nehmen sie das Beispiel einer ansteckenden Krankheit. Man kann sich vor der Krankheit nicht impfen lassen. Wenn man die Erkrankung jedoch einmal durchstanden hat, ist man immun. Die zwei Wege Vorbeugen und Heilen haben ein unterschiedliches Ziel. Man kann die beiden Wege daher kaum miteinander vergleichen. Unter Umständen ist das Vorbeugen sogar so aufwändig, dass es einfacher ist die Erkrankung einmal über sich ergehen zu lassen.

Bei Konflikten sind Ausgangspunkt und Ziel nie gleich. Ein Konflikt hinterlässt bei den betroffenen immer Spuren und beeinflusst ihr zukünftiges Verhalten. Vorbeugen im medizinischen Sinn bedeutet in vielen Fällen Aufschieben. Man kann eine Erkältung durch vorbeugende Maßnahmen nicht gänzlich ausschließen. Man kann sie aber aufschieben, indem man sich im Winter wärmer anzieht. Zieht man sich nicht mehr wärmer an, erkältet man sich sehr wahrscheinlich. Der Hippokrates-Ausspruch wird zu: Verschieben ist besser als Heilen. Die These, die im Raum steht, wenn man von Konfliktprävention spricht, lautet: Verschieben ist besser als Bewältigen. In dieser Formulierung trifft das auf Konflikte leider nicht zu! Im Gegenteil, es gibt Konflikte, die sind unausweichlich und nötig: Im Rahmen der Team-Bildung werden Phasen durchlaufen, in denen Konflikte und deren Bewältigung eine wichtige Rolle spielen.<sup>41</sup> Ohne diese Konflikte kann die Entwicklung nicht weitergehen. Die zwei Wege Vorbeugen und Heilen haben in diesem Fall also zwei völlig voneinander verschiedene Ziele.

Bevor man sich also entscheidet, konfliktpräventiv tätig zu werden, muss man sich fragen: Ist es sinnvoll, den Konflikt zu vermeiden, oder sollte man besser versuchen, auf seinen Verlauf Einfluss zu nehmen?

### 3.1 Konfliktpräventive Kommunikation

Neben den unvermeidlichen Konflikten, in deren Verlauf alle Beteiligten wachsen, gibt es auch solche, die ganz sicher ohne Nutzen sind. Sie entspringen nicht der Sache selbst, sondern dem Gespräch darüber. Der Konflikt ist dann kein Konflikt

---

<sup>41</sup> Hedwig Kellner; Projekte konfliktfrei führen: Wie Sie ein erfolgreiches Team aufbauen; 2000; Hanser; ISBN 9783446214910; Seite 146 ➤

zur Sache, sondern einer über deren Präsentation: Der Ton macht die Musik, sagt der Volksmund. Um die eigenen Aussagen, mit der Forderung nach konfliktpräventiver Kommunikation in Einklang zu bringen, muss man zunächst einige Gedanken zu gängigen Schwierigkeiten machen, die dabei auftreten.

In vielen Streitgesprächen fällt irgendwann der Satz: „*Was ist eigentlich Dein Problem?*“ Dieser Satz kommt üblicherweise nicht zu Beginn des Gesprächs, sondern leider erst viel zu spät, wenn zumindest klar ist, dass nichts klar ist. Sich klar auszudrücken ist also die erste Anforderung. Was klar ist und was nicht, bestimmt in jedem Fall der Empfänger einer Nachricht. Es hilft in einem konkreten Gespräch gar nichts, wenn man sich zwar objektiv klar ausgedrückt hat, subjektiv aber nicht verstanden worden ist.

Wenn man einem Mitarbeiter in einer stundenlangen Marathon-Sitzung alle Sicherheitsregeln des Unternehmens in glasklarem deutsch präsentiert, werden diese trotzdem in einem trüben Brei verschwimmen, wenn nicht *klar* gemacht wurde, worauf es ankommt. Klarheit entsteht in diesem Fall durch eine Begrenzung aufs Wesentliche. Wesentlich ist, was im Moment wichtig ist. Für einen neuen Mitarbeiter – nennen wir ihn Marvin – ist am ersten Tag wichtig, dass er zu dienstlichen Dingen verschwiegen sein muss. Ihm zu sagen, dass Verstöße bei Personaldaten nicht nur arbeitsrechtliche, sondern auch datenschutzrechtliche Konsequenzen haben, er bei Entwicklungsgeheimnissen fristlos, bei sonstigen Interna mit Abmahnung und bei freigegebenen Daten gar nicht gekündigt wird, freigegebene Daten nur von Abteilungsleitern, oder durch diese schriftlich Beauftragte, freigegeben werden können und er diese schriftliche Beauftragung jeweils telefonisch beim zuständigen Sicherheitsbeauftragten hinterfragen muss und er, wenn er das versäumt, doch fristlos entlassen wird, bringt nichts. Konnten Sie mir folgen? Was bringt nichts? Es bringt nichts, jemanden mit mehr Informationen zu füttern, als er verkraften kann. Er wird verwirrt sein und dann sicher einiges falsch machen.

Sich knapp auszudrücken ist daher ebenso wichtig, wie sich klar auszudrücken. Diese Forderung ist jedoch nicht leicht zu erfüllen, verlangt sie doch von den Sicherheitsexperten wichtige Regelungen zunächst weg zu lassen. Wenn man eine Firewall neu startet, macht man es genauso: `INPUT, FORWARD, OUTPUT: DROP`<sup>42</sup>! Sehr klar, sehr knapp. Erst nach dieser Default Policy wird die Firewall mit den einzelnen Regeln und Ausnahmen gefüttert. Man sollte bei diesem Bild aber nicht vergessen, dass sich die Firewall alles merkt, was man ihr danach an Regeln mitgibt. Das ist bei Menschen leider nicht der Fall. Umso wichtiger ist es, die Default Policy klar und knapp zu präsentieren. Für den Mitarbeiter Marvin heißt

---

<sup>42</sup> Richtig heißt es beispielsweise bei iptables: `iptables -P INPUT DROP ; iptables -P FORWARD DROP ; iptables -P OUTPUT DROP`

die Default Policy: Verschwiegenheit in allen dienstlichen Angelegenheiten und daran muss er sich im Zweifel immer erinnern.

Ebenso wenig hilfreich ist es, wenn man mit seinen Bildern und Vergleichen daneben liegt. Durch falsche Vergleiche wird der Gesprächspartner auf eine falsche Fährte gelockt. Sicherheitsprofis verwenden oft Vergleiche in Form von Vorfällen oder Gerichtsurteilen, um zu belegen, dass eine Sicherheitsmaßnahme begründet ist. Diese Beispiele sollten den Kern der Aussage, die sie untermauern sollen auch treffen. Und auch hier gilt: Sie müssen für den Empfänger der Nachricht *subjektiv* treffend sein. Das Rosinenkuchenmodell von Joseph John Thomson ist ein Atommodell aus dem Jahre 1903 und es liegt sicher meilenweit daneben, wenn man damit seine Theorien auf dem jährlichen Workshop der Atomphysiker am Max Planck Institut untermauern will. Wenn man jedoch zum ersten Mal erklären will, dass Atome nicht atomar sind, sondern Elektronen enthalten, leistet es weiterhin gute Dienste.

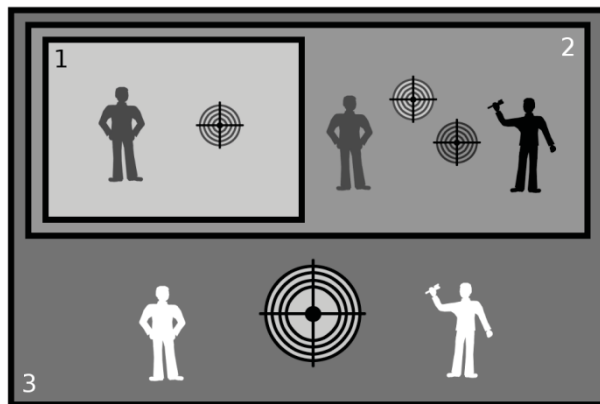


**Abbildung 3-2:** Jedem Publikum das Seine

Bisher haben wir also die drei Anforderungen klar, knapp und treffend. Für eine konfliktpräventive Kommunikation ist es jedoch noch wichtiger, nicht zu werten. Um Missverständnissen vorzubeugen: Bei einem Sicherheitsvorfall Geld zu verlieren ist schlecht und davon verschont zu bleiben ist gut; Sicherheitsverstöße sind schlecht und sich an die Regeln zu halten ist gut. Das ist mit wertfrei nicht gemeint. Es geht darum keine persönliche Wertung vorzunehmen. Jemand ist kein schlechterer Mensch, wenn er sich nicht an Sicherheitsregeln hält.

Sicherheitsverstöße sind einfach gefährlich für den Fortbestand der Firma. Im Kapitel *Willkommen auf der Security-Bühne* haben wir gesehen, dass sich für die meisten Mitarbeiter die Konzentration auf andere Bühnen richtet. Es muss klar bleiben, dass Täter, die sich menschliche Schwächen der Mitarbeiter zu Nutze machen und das Unternehmen angreifen, die schlechteren Menschen sind, und nicht die Mitarbeiter, die angegriffen werden.

Kevin Mitnick zeigt in seinem Buch *Die Kunst der Täuschung*<sup>43</sup> eindrucksvoll, mit wie viel Engagement und Ausdauer sich Angreifer auf ihren großen Auftritt auf der Security-Bühne vorbereiten. Man macht es sich zu einfach, wenn man die Mitarbeiter zu schlechteren Menschen erklärt, die durch ihr nachlässiges Verhalten diese Angriffe möglich machen. In vielen Fällen tun sie nicht einmal etwas wirklich Falsches, sondern das, was man von ihnen erwartet: Sie helfen. Angreifer die es ernst meinen, finden immer jemanden, der einen Fehler macht oder ihnen hilft – die Frage ist nur, wie lange sie dafür brauchen. Sicherheitsexperten, die einem Mitarbeiter den persönlichen Vorwurf machen, sich falsch verhalten zu haben, müssen sich immer auch fragen, ob sie selbst wirklich alles getan haben, den Mitarbeiter vor diesem Fehltritt zu bewahren. Unser Ziel war es ja, unnütze Konflikte zu vermeiden. Und ein Konflikt darüber, ob das Verhalten des Mitarbeiters nun gut oder schlecht war, führt nicht weiter. Das Verhalten des Angreifers, der die Schwäche ausgenutzt hat, war schlecht, und darauf muss sich unser Augenmerk richten. Wenn wir gemeinsam daran arbeiten wollen, dass der Fehler nicht erneut passiert, sollten wir daher auf Wertungen verzichten.

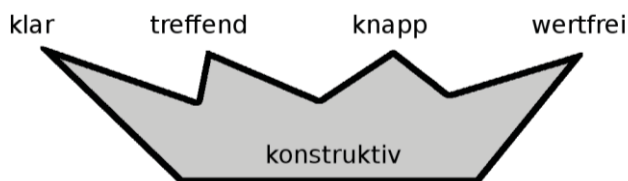


**Abbildung 3-3:** Die drei Ebenen konstruktiver Kommunikation

<sup>43</sup> Kevin Mitnick; *Die Kunst der Täuschung*; 2003; mitp; ISBN 3-8266-1569-7

Sich klar, treffend, knapp und wertfrei auszudrücken ist für IT-Sicherheitsbeauftragte, Datenschützer und Co. der Grundstein für einen Arbeitsalltag, der frei von unnützen Konflikten ist. Auf diese Art zu kommunizieren ist auf dieselbe Art präventiv, wie sich im Winter warm anzuziehen: Ein Konflikt, der entsteht, weil man sich unklar oder wertend ausgedrückt hat, ist genauso unnütz wie eine Erkältung. Eine zusätzliche Anforderung an konfliktpräventive Kommunikation ist es, konstruktiv<sup>44</sup> zu kommunizieren. Diese Anforderung überspannt die vier anderen Grundsätze und wird in drei Ebenen gegliedert (vgl. Abbildung 3-3):

1. Nehmen wir zur Verdeutlichung die folgende Aussage: *„Mein Problem ist, dass Sie meinen Zielen im Weg stehen und ich einen Weg suchen werde, diese Störung abzustellen.“* Nach allem, was wir bisher wissen ist dieser Satz klar, treffend, knapp und wertfrei. Noch ist der Satz aber alles andere als dazu geeignet, einen Konflikt zu vermeiden. Im Moment gibt es in der Aussage scheinbar nur eine Person, die legitime Ziele hat.
2. Zweifellos kann man konstruktiver werden, wenn man den Zielen der zweiten Person Raum gibt: *„Mein Problem ist, dass ich meine Ziele nicht verfolgen kann, weil Sie ein Ziel verfolgen, das meinem entgegensteht. Ich werde jedoch einen Weg suchen, diese Störung abzustellen.“* So hört es sich bereits deutlich besser an. Die Ziele der zweiten Person werden nun ebenfalls beachtet.
3. Es geht aber noch konstruktiver, wenn man ein gemeinsames Ziel definiert: *„Wir haben ein gemeinsames Problem, weil wir zur Zeit keine Idee haben, wie wir unsere gegensätzlich erscheinenden Ziele weitgehend vereinen können. Wir werden jedoch einen Weg suchen, das zu erreichen.“* In dieser Form sind alle Forderungen nach konfliktpräventiver Kommunikation erfüllt und die Aussage führt nicht in eine wenig konstruktive Sackgasse.



**Abbildung 3-4:** Die Kommunikationskrone

In Abbildung 3-4 sind alle fünf Bestandteile der konfliktpräventiven Kommunikation als Krone dargestellt. Diese bildet die Grundlage unserer

<sup>44</sup> Anne Dieter, Leo Montada, Annedore Schulze (Hrsg.); *Gerechtigkeit im Konfliktmanagement und in der Mediation*; 2000; Campus Verlag; Seite 122 ☞

Bemühungen, unnötige Konflikte zu vermeiden. Aber auch in unvermeidlichen Konflikten sind sprachliche Mindeststandards die Voraussetzung für Deeskalation. Konflikte dürfen nicht so ausgetragen werden, dass die Beteiligten nicht mehr zusammenzuarbeiten können.

## 3.2 Gemeinsames Vokabular

Wir haben gesehen, wie wichtig es ist, sich klar und treffend auszudrücken. Wer dabei noch knapp und wertfrei bleibt, hat die halbe Miete. Genauso bedeutend ist es, seine Interessen konstruktiv vorzutragen, damit es für den Gesprächspartner noch eine Möglichkeit gibt, seine Interessen einbringen zu können. Nicht zuletzt beim Versuch sich treffend auszudrücken, kommt einem gemeinsamen Vokabular eine wichtige Rolle zu – insbesondere dann, wenn Sicherheitsexperten unter sich sind. Die Sicherheits-Akteure auf der Security-Bühne sprechen leider oft nicht dieselbe Sprache und verstehen sich nicht richtig, obwohl sie sich objektiv treffend ausgedrückt haben. Aber auch in diesem Fall gilt, dass es darauf ankommt, wie der Empfänger einer Nachricht sie subjektiv versteht.

Das Problem, dass auf der Security-Bühne nicht immer alle vom selben Thema sprechen, nur weil sie dieselben Worte benutzen, ist uns im Verlauf des Buchs bereits mehrfach begegnet. Zunächst haben wir auf Seite 13 festgestellt, dass es keinen einheitlichen Branchen-Begriff gibt, auf den man sich stützen kann. Sicherheit ist der Oberbegriff für viele Branchen: Von staatlichen Behörden, wie der Polizei oder der Feuerwehr, über den Wachmann am Werkstor bis hin zu Datenschützern, IT-Sicherheitsbeauftragten und Sicherheitsbeauftragten. Im Abschnitt über die IT-Sicherheitsbeauftragten haben wir gesehen, dass zu deren Aufgaben mittlerweile deutlich mehr gehört, wie die Sicherheit der Informationstechnik (IT) und das leicht zu Missverständnissen führen kann. Was war noch schnell der Unterschied zwischen IT-, IV-, IS- und I-Sicherheit?

Regelmäßig kommt es zwischen den Sicherheitsexperten in einem Unternehmen oder einer Behörde zu Reibereien oder Missverständnissen, weil sie unterschiedliche Auffassungen von Sicherheit haben und davon, wie weit der Begriff ausgelegt werden soll. Wir müssen uns also im Folgenden das Security-Vokabular etwas genauer ansehen. Wenn Datenschutz Ihr Schwerpunkt ist, muss ich Ihnen natürlich nicht erklären, was darunter zu verstehen ist. Für den Sicherheitsbeauftragten Dave aus der ExAmple AG ist es aber wichtig, den Begriff genauer kennen zu lernen. Wenn Sie andererseits IT-Sicherheitsbeauftragter sind, hilft es Ihnen weiter, eine bessere Vorstellung vom Begriff Corporate Security zu bekommen. Als Leiter des Werkschutzes ist es Ihnen eventuell noch nicht ganz klar, welche Bestandteile alle zu einem Informationssystem gehören können.

Am Ende dieses Abschnitts stehen natürlich keine unumstößlichen Begriffs-Prototypen, mit denen Sie in jedem Gespräch richtig liegen. Sie werden jedoch nach der Lektüre ein Gespür für die begrifflichen Nuancen haben und in Zukunft schnell merken, wann ein Missverständnis im Raum steht, dass Sie mit zwei, drei gezielten Fragen aus der Welt schaffen können. Beginnen wir mit dem Begriff des Informationssystems.

### 3.2.1 Informationssysteme

Die Definition des Begriffs *Informationssysteme* beginnt mit der Klärung der ersten Worthälfte: Information. Auch die anderen Begriffe, die wir noch unter die Lupe nehmen werden, haben mit Information zu tun. Sie denken vielleicht, dass die Antwort ganz einfach sein sollte – ist sie aber nicht. Das Wort *Information* ist sogar so schwer abzugrenzen, das es als Beispiel für schlechte und umstrittene Wikipedia-Artikel dienen kann<sup>45</sup>. Dort heißt es in der Einleitung: „Die Information verliert, sobald sie informiert hat, ihre Qualität als Information: News is what’s different.“ Zitiert wird dabei aus einem Buch<sup>46</sup> über Journalismus, dass auf diese Art den Begriff der Nachricht definiert.



Abbildung 3-5: Alles eine Frage der richtigen Wortwahl

<sup>45</sup> <http://de.wikipedia.org/w/index.php?title=Information&oldid=65157271>; eingesehen am 02.10.2009

<sup>46</sup> Walter von La Roche; Einführung in den praktischen Journalismus; 18. Aktualisierte und erweiterte Auflage 2008; Econ; ISBN: 978-3-430-20045-5; Seite 75

Auch auf der Diskussionsseite zu dem Artikel geht es heiß her: *„Dieser Artikel ist äußerst konfus“*, oder *„Der Abschnitt zur Informationstheorie war sachlich grob falsch.“* Oder: *„Der ganze Text baut auf der veralteten Sicht auf und kann eigentlich in die Tonne!“* Inmitten der Negativ-Stimmen findet man einen Antrag, den Artikel in die Liste der lesenswerten Wikipedia-Artikel aufzunehmen – nicht jeder findet die Sichtweise des Artikels also *äußerst konfus* oder *grob falsch*.

Wie hilft uns das schlechte Bild, das der Wikipedia-Artikel abgibt, bei der Erörterung von Security-Konflikten weiter? Stellen Sie sich vor, der IT-Sicherheitsbeauftragte der ExAmpLe AG Bob spricht mit verschiedenen Personen und benutzt dabei seine Sichtweise auf den Begriff *Information* – ihm würden unter Umständen dieselben Bewertungen entgegenschlagen, wie auf der Diskussionsseite in der Wikipedia: *„äußerst konfus“*, *„grob falsch“*, *„kann eigentlich in die Tonne!“*

Der Satz *„Die Information verliert, sobald sie informiert hat, ihre Qualität als Information“*, ist natürlich kein guter Ansatz für einen Security-Experten. Das vertrauliche Dokument bleibt ja weiterhin vertraulich, auch wenn es schon jemand gelesen hat. Im Rahmen der militärischen Geheimhaltung geht das sogar soweit, dass für jedermann zugängliche Fakten, trotzdem in der höchsten Geheimhaltungsstufe eingruppiert bleiben: Die Stationierungsorte von Atomwaffen sind leicht herauszubekommen. Überall in der Presse wird darüber berichtet. Intern bleiben die Orte weiterhin TOP SECRET. Für den Leser einer Zeitung macht es wohl keinen Unterschied, ob er in der Zeitung liest, dass auf dem Fliegerhorst Büchel Atomwaffen stationiert sind – was jeder weiß – oder in einem internen Dokument, dass ein Offizier in einem Zug liegengelassen hat. Für den zuständigen Sicherheitsbeauftragten macht das aber einen erheblichen Unterschied.

Für Sicherheitsexperten ist daher gar nicht so wichtig, ob eine Information nach wissenschaftlichen Maßstäben als solche bezeichnet werden kann. Es reicht, wenn jemand dem Sicherheitsbeauftragten sagt, dass etwas als Information zu behandeln ist. Ist ein Haus eine Information? Eher nicht. Wenn das Haus jedoch in Berlin-Mitte steht und dort voraussichtlich 2011 der Bundesnachrichtendienst (BND) einzieht, sieht das schnell anders aus. Eine Information kann für einen Sicherheitsexperten eine ganze Menge sein und er kann nicht selbst oder mit Hilfe von wissenschaftlichen Definitionen bestimmen, wie man eine Information von einer Nicht-Information abgrenzt.

Sich dem Begriff Informationssystem von der Seite der Informationen zu nähern ist also mit gewissen Schwierigkeiten verbunden. Leichter machen es sich diejenigen, die zuerst nach den *Systemen* fragen. Auch für sie ist nicht wirklich entscheidend, was Informationen sind. Im Mittelpunkt stehen die Systeme, mit denen die Informationen *verarbeitet*, *gespeichert* oder *übertragen* werden: Die Informationen

sind sicher, wenn die Systeme sicher sind. Dem Sicherheitsbeauftragten, der die Geheimhaltung des Gebäudeplans für das BND-Gebäude sicherstellen soll, hilft das natürlich nicht weiter. Es ist ja schön und gut, wenn niemand an die Pläne auf dem Server kommt, aber während des Baus jeder ins Gebäude kommt bzw. den Grundriss von oben aus einem Flugzeug abfotografieren kann.

Informationssysteme sind also mehr als nur die Summe ihrer Teile. Sie bestehen nicht ausschließlich aus Informationen oder Technik. Informationssysteme sind sozio-technische Gesamtsysteme, die aus Informationen, Hardware, Software und aus den beteiligten Menschen bestehen. Was Informationen sind und ob sie zu schützen sind, muss sich folglich aus dem Gesamtsystem ableiten.

In der Literatur wird der Begriff des Informationssystems nicht immer so weit gefasst. Bei Fischer<sup>47</sup> werden Informationssysteme beschrieben als *„Datenorganisationsformen auf Rechenanlagen, die bestimmte Vorgänge und Abläufe in Kommunikationsprozessen unterstützen“*. Bei Hansen<sup>48</sup> wird der Mensch zwar in die Begriffsdefinition einbezogen, steht der Technik jedoch quasi gegenüber. Nach der dortigen Definition ist *„ein Informationssystem eine Menge von Menschen und Maschinen (Automaten), die Informationen erzeugen und/oder benutzen und die durch Kommunikationsbeziehungen miteinander verbunden sind“*. Verschiedene andere Autoren<sup>49</sup> verwenden den Begriff eines aus Teilsystemen bestehenden sozio-technischen Gesamtsystems. Dies ist eine Begrifflichkeit, die stärker auf verbindende, soziale Elemente setzt und nicht versucht, den Begriff in eine kurze Formel zu pressen.

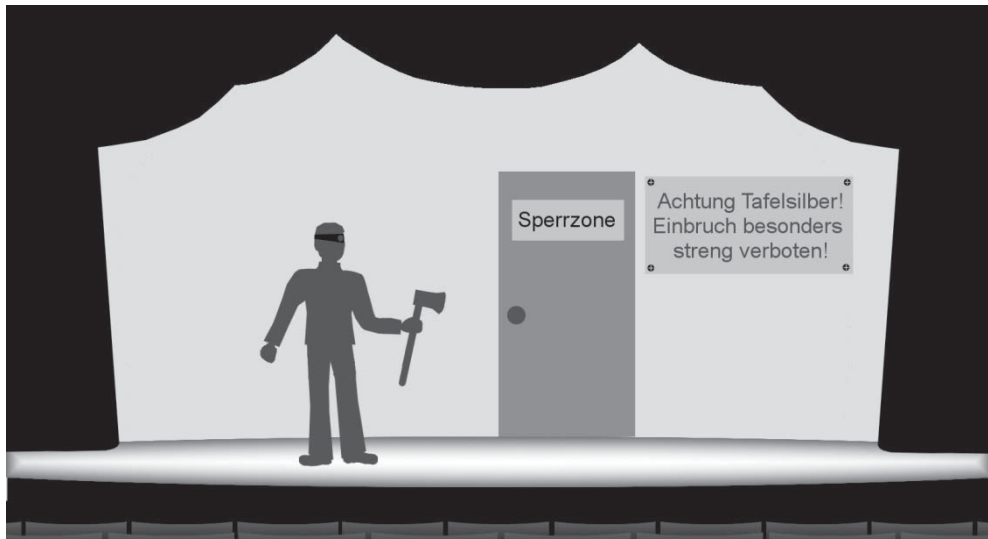
Besonders wichtig sind die Verknüpfungen innerhalb eines Informationssystems, die man gar nicht hoch genug einschätzen kann. Wer die Bauvorschriften kennt, die für eine Zaunanlage um ein Atomwaffenlager gelten, der kann anhand des Zauns sagen, was in den Bunkieranlagen gelagert wird. Den Serverraum in einem Gebäude findet man leicht, wenn man sich an den Außengeräten der Klimaanlage orientiert und hinter vergitterten Fenstern befinden sich nicht nur Gefängniszellen. Auf diese Art werden Zäune, Klimageräte und Fenstergitter leicht zu einem Informationsschild mit der Aufschrift: *„Für größtmöglichen Schaden bitte hier einbrechen!“*

---

<sup>47</sup> Fischer, Joachim; Informationswirtschaft: Anwendungsmanagement; 1999; Oldenbourg, ISBN 3486250787

<sup>48</sup> Meyer, H.-M.: Softwarearchitekturen für verteilte Verarbeitung. In: Hansen, W.-R.: Client-Server-Architektur; 1993; Addison-Wesley

<sup>49</sup> Helmut Krcmar: Informationsmanagement. Springer, Berlin 2000 oder Stefan Kirn: IV-Strategie, Hagen 2007



**Abbildung 3-6:** Nicht jeder lässt sich von Verboten abhalten – im Gegenteil!

Am Ende des Abschnitts 3.2 werde ich eine Frage stellen, die deutlich macht, wie wichtig es ist, sich im eigenen Unternehmen oder in der Behörde darüber klar zu werden, wie weit man die einzelnen Begriffe auslegt und wie groß das Konfliktpotential ist, dass hinter dieser Auslegung verborgen liegt.

### 3.2.2 Sicherheit

Was für den Begriff des Informationssystems gilt, gilt auch für den Begriff der Sicherheit. Unter Sicherheit versteht fast jeder etwas anderes. Das liegt daran, dass wir im Deutschen für viele verschiedene Dinge nur dieses eine Wort benutzen, obwohl wir durchaus viele andere zur Auswahl hätten. Dadurch wird mittlerweile so einiges als gesichert bezeichnet. Nehmen wir als Beispiel die folgenden Sätze:

- ❖ „Wir müssen diese Erkenntnis absichern.“
- ❖ „Wir müssen diesen Server absichern“

Eine Erkenntnis abzusichern ist natürlich etwas anderes, wie einen Server abzusichern, auch wenn es dasselbe Wort im selben Satz ist. Wenn Sie das Beispiel zu plump finden, dann tauschen Sie im ersten Satz das Wort *Erkenntnis* gegen *Daten* aus:

- ❖ „Wir müssen diese Daten absichern.“

Meinen Sie, es macht einen Unterschied, ob der Satz von einem Statistiker oder von einem Datenschützer stammt? Nicht jeder versteht unter Datensicherheit dasselbe und doch sagen alle aus ihrer Perspektive das Richtige.

Es gibt im Deutschen eine Unmenge an Synonymen für das Wort *sicher*: gewiss, gefahrlos, risikolos, zuverlässig, geschützt, unbedroht, besiegelt, beweisbar, garantiert, erwiesen, erprobt, zuverlässig, unverwundbar, bewacht, blockiert, verlässlich, etc. Versuchen Sie vor diesem Hintergrund folgenden Satz zu verstehen: „Die Daten auf unseren Servern sind sicher.“ Das geht einfach nicht. Probieren Sie die Synonyme im Geiste durch. Es ist eben ein erheblicher Unterschied, ob die Daten unbedroht sind, ob sie geschützt sind, oder ob von ihnen keine Gefahr ausgeht. Ohne diese Unterscheidungen kann man unmöglich ein Gespräch führen, dass ohne Missverständnisse bleibt.

### 3.2.2.1 In English please:

certainty, safety, security, protection, privacy etc.

Eines kann man mit ziemlicher Gewissheit (certainty) sagen: Wo das Deutsche oberflächlich bleibt, unterscheidet das Englische glücklicherweise. Es gibt z.B. keine functional security, sondern safety und wo im Deutschen der Begriff Datensicherheit viele Fragen aufwirft, gibt es im Englischen security, protection und privacy.

Wenn man den Begriff Sicherheit nach den Anforderungen nach konfliktpräventiver Kommunikation von Seite 66 treffend verwenden will, so muss man ihn erläutern. In technischen Konzepten oder bei Gesprächspartnern mit Englischkenntnissen eignen sich die englischen Begriffe dafür ganz gut. In ihrem Standardwerk *IT-Sicherheit* geht Claudia Eckert nach diesem System vor und lässt damit wenig Fragen offen.<sup>50</sup> Im Folgenden gehen wir diese Begriffe durch. Teilweise gibt es auch deutsche Begriffe, die für den entsprechenden Blickwinkel treffender sind, als das Wort *sicher*. Diese Auflistung soll keine Werbung für Anglizismen sein, sie hilft jedoch ungemein, das Verständnis für die Gefahr von Missverständnissen um den Sicherheitsbegriff zu schärfen.

**Safety:** Hier würden wir im Deutschen etwa *Funktionssicherheit* oder *Betriebssicherheit* sagen. Funktionssicher heißt, dass die Ist-Funktionalität mit der Soll-Funktionalität übereinstimmt, das System also richtig funktioniert. Betriebssicher heißt kurz gesagt: Man kann sich nicht verletzen oder ähnliches.

---

<sup>50</sup> Claudia Eckert; *IT-Sicherheit* Studienausgabe; 2005; Oldenbourg; ISBN: 3-486-57676-3; Seite 4 ff

Man sollte voraussetzen, dass so etwas in der Soll-Funktionalität ausgeschlossen wurde.

**Security:** Zu Deutsch etwa *Informationssicherheit*. So bezeichnet man ein Informationssystem, das nur solche Zustände annimmt, die zu keiner unerlaubten Informationsveränderung oder Informationsgewinnung führen.

**Protection:** Hier wird es schon schwerer eine deutsche Entsprechung zu finden. Der Begriff *Datensicherheit* kommt der Bedeutung am nächsten. Gemeint ist die Eigenschaft eines Informationssystems, nur solche Zustände anzunehmen, die keinen unerlaubten Zugriff auf Daten und Systemressourcen erlauben. *Daten* meint hier nicht die Daten im Sinne des Datenschutzgesetzes, sondern Daten im Sinne der Informatik. Zu dieser *Datensicherheit* gehört auch die *Datensicherung*, also das Anfertigen von Backups.

Das englische Wort *Protection* trifft es einfach besser wie *Datensicherheit* plus *Datensicherung*. Vorsicht! Fußnote 51 könnte mehr verwirren, als sie nutzt!<sup>51</sup>

**Privacy:** Das ist einfach zu übersetzen: *Datenschutz*. Wer Datenschutzbeauftragter ist, kann sich jetzt freuen, weil gesetzlich geregelt ist, was er meint, wenn er von Datenschutz spricht. Das ist ein deutlicher Vorteil gegenüber den IT-Sicherheitsbeauftragten.

Die ersten vier Begriffe ergeben zusammen in etwa das, was wir von einem sicheren Informationssystem erwarten: Funktionssicherheit, Betriebssicherheit, Informationssicherheit, Datensicherheit, Datensicherung und Datenschutz. Darüberhinaus werden sogenannte Schutzziele definiert, die für zu schützende Daten und Informationen gelten sollen:

**Authenticity:** Gemeint ist die *Echtheit* und *Glaubwürdigkeit* eines Objekts, die sich mit charakteristischen Eigenschaften überprüfen lässt.

---

<sup>51</sup> Eigentlich müsste man *Protection* mit *Schutz* übersetzen. Dann hätte man zu Deutsch *Datenschutz* und läge komplett daneben, weil der Datenschutz in den Datenschutzgesetzen geregelt ist und etwas ganz anderes meint: *Privacy*. Wenn Sie die Verwirrung komplett machen wollen, tauschen Sie *Daten* gegen *Informationen*, dann haben Sie *Informationssicherheit*. So hatten wir aber leider schon *Security* übersetzt.

- Integrity:** Die *Manipulationssicherheit* eines Systems schließt die unerlaubte und unbemerkte Veränderung aus (vgl. Security).
- Confidentiality:** Die *Vertraulichkeit* eines Systems schließt eine unerlaubte Informationsgewinnung aus (vgl. Security).
- Availability:** Die *Verfügbarkeit* eines Systems oder Teilsystems ist gewährleistet, wenn deren berechnigte Nutzung nicht unerlaubt beeinträchtigt werden kann.
- Non Repudiation:** *Verbindlichkeit* oder auch *Nicht-Abstreitbarkeit* liegt vor, wenn innerhalb des Informationssystems Aktionen im Nachhinein eindeutig zuzuordnen sind und nicht abgestritten werden können.

In Tabelle 3-1 sind die Begriffspaare noch einmal übersichtlich gegenübergestellt und unter den zwei Oberbegriffen Sicherheit und Sicherheitsziele zusammengefasst.

| Englisch        | Deutsch                                 | Oberbegriff           |
|-----------------|-----------------------------------------|-----------------------|
| Safety          | Funktionssicherheit, Betriebssicherheit | Begriff<br>Sicherheit |
| Security        | Informationssicherheit                  |                       |
| Protection      | Datensicherheit, Datensicherung         |                       |
| Privacy         | Datenschutz                             |                       |
| Authenticity    | Echtheit, Glaubwürdigkeit               | Sicherheitsziele      |
| Integrity       | Manipulationssicherheit                 |                       |
| Confidentiality | Vertraulichkeit                         |                       |
| Availability    | Verfügbarkeit                           |                       |
| Non Repudiation | Verbindlichkeit, Nicht-Abstreitbarkeit  |                       |

**Tabelle 3-1:**      Englisch und deutsches Sicherheitsvokabular

### 3.2.2.2 Gegenüberstellung: Datenschutz vs. Informationssicherheit

Ob Datenschutz/ Privacy oder Informationssicherheit/ Security: Mit diesen Begriffen werden unterschiedliche Ziele verfolgt. Der Datenschutz schützt das Recht auf freie informationelle Selbstbestimmung aus dem Grundgesetz und im

Rahmen der Informationssicherheit ist Datenschutz meist nur ein zufälliges Nebenprodukt. Oft genug werden die Begriffe von allen Beteiligten munter miteinander gemischt.

Im Bereich der öffentlichen Verwaltung stößt man immer wieder auf das Missverständnis, dass in Systemen, in denen Informationen einer hohen Verschlusssachen-Einstufung verarbeitet werden dürfen – z.B. GEHEIM – auch unbeschränkt Personaldaten bearbeitet werden können. Offensichtlich herrscht dort die Meinung vor, dass ein System, das für Staatsgeheimnisse taugt, für den Datenschutz lange gut ist. So ist es aber nicht. Der Datenschutz schützt die Daten des Individuums vor Offenlegung, während der Geheimschutz Staatsgeheimnisse vor Offenlegung schützt. Was jeweils unter Offenlegung zu verstehen ist, bestimmt im einen Fall der Besitzer der Daten, nämlich das Individuum, und im anderen Fall der Besitzer der Geheimnisse, nämlich der Staat.

Derartige Missverständnisse sind genauso wenig selten, wie sie für die betroffenen Sicherheitsexperten nachzuvollziehen sind. Was jemandem einleuchtet, der sich täglich mit Datenschutz- und Security-Fragen auseinandersetzt, erschließt sich den normalen Anwendern meist nicht einmal auf den zweiten Blick. Bei der Verwendung der Begriffe Datenschutz oder Informationssicherheit muss man diese daher immer erklären oder sich zumindest rückversichern, dass dem Gesprächspartner der Unterschied der beiden Ansätze auch bewusst ist. Dazu gehört es, die Zweideutigkeit des Begriffs *Daten* stets zu berücksichtigen. Für einen Datenbankadministrator sind Daten eben etwas anderes wie für einen Datenschutzbeauftragten.

Diese Mehrdeutigkeit der Begrifflichkeiten findet sich überall in der Sicherheitsbranche und mit ihr umzugehen ist sehr schwer. Wenn Sie die Bezeichnung *Sicherheits-Branche* der Bezeichnung *Security-Branche* gegenüberstellen und dabei Tabelle 3-1 zugrunde legen, bemerken Sie das Problem: Im Sinne dieser Tabelle umfasst die Security-Branche nur einen Teil der Sicherheitsbranche, nämlich die Informationssicherheits-Branche. Eine solche Unterscheidung gibt es aber in der Praxis nicht. Was konkret gemeint ist, hängt im Einzelfall von Nuancen ab. Wenn sich also noch nicht einmal die Fachleute auf ein schlüssiges Vokabular einigen können, wie soll man da von all den anderen Protagonisten auf der Security-Bühne erwarten, jeden Satz so zu verstehen, wie er gemeint ist? Man kommt daher nicht umhin, sich im Unternehmen oder der Behörde auf einen gemeinsamen Begriffs-Pool zu verständigen. Dazu gehört auch, zu klären, wo Datenschutz aufhört, wo Informationssicherheit anfängt und wo es Überschneidungen gibt.

### 3.2.3 Die Sicherheitspräfixe IT, IV, IS und I

Um den geschilderten Problemen Herr zu werden, ist es in vielen Fällen hilfreich, dem missverständlichen Begriff *Sicherheit* die Präfixe IT, IS, IV und I voranzustellen. Diese Reihe von präziseren Begriffen haben wir bereits auf Seite 23 kennengelernt. IT steht für Informationstechnik, IV für Informationsverarbeitung, IS für Informationssystem und I für Information. Im Folgenden werden diese Begriffe mit dem bisher erarbeiteten Sicherheitsvokabular in Zusammenhang gebracht und in Tabelle 3-2 gemeinsam dargestellt. Wenn Sie die Tabelle beim Lesen der nächsten Absätze im Auge behalten, werden die folgenden Beispiele deutlicher.

- ❖ Unter dem Begriff *IT-Sicherheit* versteht man klassisch die Sicherheit der Informationstechnik. Im Abschnitt über die IT-Sicherheitsbeauftragten haben wir jedoch gesehen, dass sich dieser Bereich im Laufe der Zeit immer mehr vergrößert hat und mehr und mehr das gesamte Informationssystem betrifft. Unter IT-Sicherheit fasst man nicht mehr nur Datensicherheit und Datensicherung zusammen. Die Funktions- und Betriebssicherheit der Anlagen gehören mittlerweile ebenso zum Aufgabenbereich, wie der über die Technik hinaus gehende Schutz der Informationen im Rahmen der Informationssicherheit. Einzig den Datenschutz grenzt man klar von der IT-Sicherheit ab. Dies mag zum einen an dem bereits zitierten Urteil des Bundesarbeitsgerichts liegen, nach dem eine EDV-Fachkraft nicht zugleich Datenschutzbeauftragter sein kann. Im Leitsatz zum Gerichtsbeschluss heißt es: *„Bedenken gegen die Zuverlässigkeit können sich daraus ergeben, dass der Arbeitnehmer neben seiner Aufgabe als Datenschutzbeauftragter Tätigkeiten ausübt, die mit seiner Kontrollfunktion unvereinbar sind, weil sie den Arbeitnehmer in einen Interessenkonflikt geraten lassen.“*<sup>52</sup> Dieser Argumentation lässt sich natürlich analog für einen IT-Sicherheitsbeauftragten formulieren. Für die IT-Sicherheit sind personenbezogene Daten einfach eine weitere Kategorie schutzbedürftiger Informationen, für die Maßnahmen der IT-Sicherheit umzusetzen sind. Und für den Datenschutz ist die IT-Sicherheit Erfüllungsgehilfe für die Herstellung der Sicherheit der elektronisch verarbeiteten personenbezogenen Daten.
- ❖ Mit *IV-Sicherheit*, also der Sicherheit der Informationsverarbeitung wird meist nur ein kleiner Teil der gesamten Sicherheit gemeint. Der Begriff wird im Alltag selten auftauchen, hat jedoch durchaus seine Berechtigung. Er ist besonders für technisches Personal, wie z.B. Datenbank-Administratoren von

---

<sup>52</sup> BAG; Beschluss des 1. Senats; Mitbestimmung des Betriebsrates bei Versetzung eines Datenschutzbeauftragten; 22.03.1994; Aktenzeichen: 1 ABR 51/93 ☞

Bedeutung, deren Augenmerk auf die Verarbeitung von Informationen gerichtet ist. Dieser Ansatz ist sehr pragmatisch und befasst sich mit den Veränderungen, denen eine Information in ihrem Lebenszyklus unterworfen ist. Diese Veränderungen lassen sich danach unterscheiden, in welcher Art die Informationen verändert werden.<sup>53</sup> Man unterscheidet die drei Arten Transmission (räumliche Veränderung, gleicher Inhalt), Translation (Veränderung der Form, gleicher Inhalt) und Transformation (Veränderung des Inhalts). Vor diesem Hintergrund erscheint es einleuchtend, dass sich die IV-Sicherheit hauptsächlich auf Maßnahmen zur Funktions- und Betriebssicherheit, Datensicherheit und eine funktionierende Datensicherung bezieht. Mit Hilfe der englischen Vokabeln kürzer: Safety und Protection. IV-Sicherheit fragt nicht, warum etwas mit den Informationen passiert, und ob es passieren sollte, sondern nur danach, ob es richtig passiert. Daher ist IV-Sicherheit ein Teil der IT-Sicherheit.

- ❖ Je nach Auslegung des Begriffs Informationssystem wird die *Informationssystem-Sicherheit* synonym mit IT-Sicherheit verwendet. Spätestens hier sollte deutlich werden, wie wichtig die zugrunde liegenden Begriffe beim gegenseitigen Verständnis sind. Nach der hier präferierten, weiter gefassten Sichtweise eines sozio-technischen Gesamtsystems versteht sich, dass auch die Maßnahmen zum Schutz personenbezogener Daten hinzuzurechnen sind. Damit gehören zur *IS-Sicherheit* alle Vokabeln des Oberbegriffs Sicherheit aus Tabelle 3-1. Das weiter gefasste Verständnis eines Informationssystems beinhaltet alle technischen Systeme, die beteiligten Menschen und insbesondere deren Kommunikationsverbindungen untereinander und nach außen. In einem solchen Informationssystem kommt man natürlich nicht umhin, alle Sicherheitsziele für alle Bestandteile der Sicherheit in Betracht zu ziehen. IS-Sicherheit beinhaltet dementsprechend – nicht nur begrifflich – auch alle Maßnahmen zur Informationssicherheit.
- ❖ Auch die *Informationssicherheit* kann aus einem engeren und einem weiteren Begriffsverständnis heraus betrachtet werden. Bei einer engen Auslegung ist sie gleichbedeutend mit dem englischen Begriff Security, wie weiter oben bereits dargestellt. Fasst man den Begriff weiter, so gehören auch Protection und Privacy hinzu. Daher verwundert es auch nicht, dass in den IT-Grundschutz-Katalogen ein Baustein Datenschutz<sup>54</sup> aufgenommen wurde. Auf Seite 22 wurde bereits geschildert, dass der IT-Grundschutz sich im Laufe der

---

<sup>53</sup> Arnold Picot, Ralf Reichwald, Rolf T. Wigand; Die grenzenlose Unternehmung: Information, Organisation und Management: Lehrbuch zur Unternehmensführung im Informationszeitalter; 2003; Gabler; ISBN 9783409522144; Seite 61 ff ↗

<sup>54</sup> Bundesamt für Sicherheit in der Informationstechnik; IT-Grundschutzbaustein 1.5 Datenschutz; [www.bsi.bund.de/grundschutz/baustein-datenschutz](http://www.bsi.bund.de/grundschutz/baustein-datenschutz)

Zeit von einem IT-Sicherheitsstandard zu einem Informationssicherheitsstandard entwickelt hat. An anderer Stelle heißt es dort: „Die Verantwortung für Informationssicherheit verbleibt in jedem Fall bei der obersten Managementebene, die Aufgabe „Informationssicherheit“ wird allerdings typischerweise an einen Beauftragten für Informationssicherheit delegiert. In den IT-Grundsatz-Dokumenten wird diese Rolle häufig als IT-Sicherheitsbeauftragter bezeichnet, auch wenn deren Aufgaben über pure IT-Sicherheit hinausgehen.“<sup>55</sup>

Immer wieder zeigt sich, wie schwer die Begriffe voneinander abzugrenzen sind, obwohl sie doch so unterschiedlich in der Bedeutung sind. Dieser Versuch gleicht dem Problem des Gordischen Knotens. Das zeigt sich besonders gut beim letzten Beispiel aus dem IT-Grundsatz: Das BSI proklamiert den IT-Grundsatz als die Basis für Informationssicherheit. Darin enthalten ist ein Baustein *Datenschutz*, für den eine Rolle *Datenschutzbeauftragter* eingeführt wird. Die Rolle des Informationssicherheitsbeauftragten heißt der Einfachheit halber IT-Sicherheitsbeauftragter. Im Datenschutzbaustein kommt er kaum vor. Die Argumentation, nach der IT-Sicherheit und Datenschutz nicht vereinbar sind, hatten wir bereits weiter oben besprochen – hier geht man in der Wortwahl über diesen Ausschluss hinweg: Für das *Datenschutzmanagement* sind die Rollen *Datenschutzbeauftragter* und *Informationssicherheitsmanagement* verantwortlich, letztere oft als IT-Sicherheitsmanagement bezeichnet, womit sich der Kreis schließt.

Die hier vorgestellten Begriffe unterlagen in der Vergangenheit einem stetigen Wandel ihrer Bedeutungen, der zum jetzigen Zeitpunkt noch nicht abgeschlossen ist. Auch für die Zukunft wird sich das Verständnis der hinter den Begriffen verborgenen Konzepte an die Herausforderungen der Zeit anpassen müssen. Die Trennlinien zwischen Technik auf der einen und dem Mensch auf der anderen Seite verlieren nach und nach an Schärfe. Es bleibt abzuwarten, ob sich am Ende der Entwicklung ein klarer Sicherheitsbegriff herauskristallisiert, oder ob sich klar abgegrenzte Teildisziplinen entwickeln. Daher kann die in Tabelle 3-2 vorgenommene Einteilung auch keinen Anspruch auf Vollständigkeit erheben. Sie dient ausschließlich dazu, sich der Idee eines gemeinsamen Vokabulars anzunähern, um Missverständnissen in der Kommunikation vorzubeugen.

---

<sup>55</sup> Bundesamt für Sicherheit in der Informationstechnik; BSI-Standard 100-2 IT-Grundsatz-Vorgehensweise; 2008; Seite 11 

| Englisch        | Deutsch                                    | Oberbegriff      | Sicherheitspräfixe |               |               |              |
|-----------------|--------------------------------------------|------------------|--------------------|---------------|---------------|--------------|
| Safety          | Funktionssicherheit,<br>Betriebssicherheit | Sicherheit       | IT-Sicherheit      | IV-Sicherheit | IS-Sicherheit |              |
| Protection      | Datensicherheit,<br>Datensicherung         |                  |                    |               |               | I-Sicherheit |
| Security        | Informationssicherheit                     |                  |                    |               |               |              |
| Privacy         | Datenschutz                                |                  |                    |               |               |              |
| Authenticity    | Echtheit,<br>Glaubwürdigkeit               | Sicherheitsziele | IT-Sicherheit      | IV-Sicherheit | IS-Sicherheit | I-Sicherheit |
| Integrity       | Manipulationssicherheit                    |                  |                    |               |               |              |
| Confidentiality | Vertraulichkeit                            |                  |                    |               |               |              |
| Availability    | Verfügbarkeit                              |                  |                    |               |               |              |
| Non Repudiation | Verbindlichkeit,<br>Nicht-Abstreitbarkeit  |                  |                    |               |               |              |

**Tabelle 3-2:** Gemeinsames Vokabular der Sicherheitsexperten

### 3.2.4 Corporate Security

Corporate Design, Corporate Governance, Corporate Social Responsibility – fast jede Disziplin unternehmerischen Handelns gibt es heute mit der Ergänzung *Corporate*. Und so gibt es natürlich mittlerweile den Begriff der Corporate Security – Unternehmenssicherheit<sup>56</sup>. Es wird versucht, mit diesem Begriff alle Tätigkeiten, die im Zusammenhang mit der Gefahrenabwehr stehen, unter einem Dach zusammenzufassen.

<sup>56</sup> Z.B.: Klaus-Rainer Müller; Handbuch Unternehmenssicherheit: Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System; 2005; Vieweg+Teubner; ISBN: 9783528058890

*The manager's handbook for corporate security*<sup>57</sup> führt dazu anhand eines Fallbeispiels einen Corporate Security Manager ein, zu dessen Zuständigkeitsbereich eine ganze Reihe von Sicherheitsfunktionen gehört, u.a.:

- ❖ Physikalische Sicherheit
- ❖ Personelle Sicherheit
- ❖ Sicherheitsausbildung und Awareness
- ❖ Brandschutz
- ❖ Notfallplanung
- ❖ Staatlicher Geheimschutz
- ❖ Informationssicherheit
- ❖ Veranstaltungssicherheit
- ❖ Etc.

Diesen umfassenden Sicherheitsansatz finden wir auch im *Handbuch Unternehmenssicherheit* wieder, in dem der Autor auch Lizenzmanagement, Projektmanagement oder Finanzmanagement zu den Aufgaben der Sicherheitsexperten hinzuzählt.

Mit einem derartig weit gesteckten Verständnis von Sicherheit gibt es nahezu keinen Bereich im Unternehmen oder der Behörde, in dem die Sicherheitsexperten nicht zuständig wären. Man kann sich leicht vorstellen, welche Auswirkungen es hat, wenn diese umfassenden Mitspracherechte in der Organisationsstruktur in einer Stelle zusammengeführt würden und welche hohen Anforderungen an jemanden zu stellen wären, der diese Stelle besetzt. Insbesondere kann man sich den Widerstand derer vorstellen, die sich von dieser Person in die Karten schauen lassen müssten.

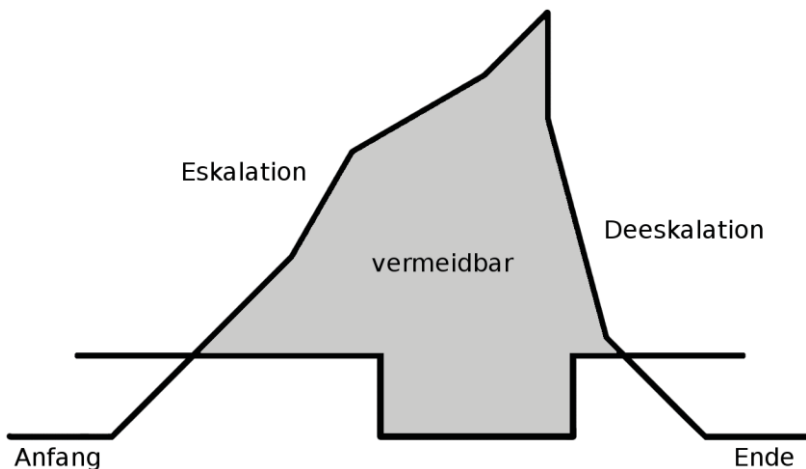
Am Ende von Abschnitt 3.2.1 hatte ich angekündigt, dass sich an der Auslegung der Sicherheitsbegriffe eine Frage festmacht, die großes Konfliktpotential beinhaltet. Nämlich die Frage danach, wie viel Einfluss die Sicherheitsexperten innerhalb einer Organisation haben sollen. Daher ist es auch so wichtig, sich im eigenen Unternehmen oder in der Behörde darüber klar zu werden, wie weit man die einzelnen Begriffe auslegt. Tut man das nicht, sind die Verteilungskonflikte vorprogrammiert.

---

<sup>57</sup> Z.B.: Gerald L. Kovacich, Edward P. Halibozek; *The manager's handbook for corporate security: establishing and managing a successful assets protection program*; 2003; Butterworth-Heinemann; ISBN: 9780750674874 

### 3.3 Konfliktpipeline

Vielfach geht es bei der Prävention von Konflikten nicht darum, sie auf unbestimmte Zeit aufzuschieben, sondern die Konfliktsamplitude zu senken und die Konfliktdauer zu verkürzen. Diese Art von Prävention ähnelt einer Impfung: Man wird zwar mit dem Krankheitserreger infiziert, aber in abgeschwächter Form. Es empfiehlt sich also auf dem Weg durch die unvermeidlichen Konflikte strukturiert und planvoll vorzugehen, um – ähnlich wie bei einer Impfung – den Konflikt gerade auf dem Level auszutragen, das nötig ist um den anvisierten Zustand zu erreichen, der nach einem bewältigten Konflikt steht. Die unnötige Eskalation muss ebenso verhindert werden, wie eine unnötige zeitliche Ausdehnung des Konflikts.



**Abbildung 3-7:** Vermeidbare Konfliktanteile

Abbildung 3-7 zeigt unter anderem diese vermeidbaren Konfliktanteile. Zunächst gibt es in jedem Konflikt einen Anfang und ein Ende, also einen Zustand, vor dem Konflikt und einen Zustand nach dem Konflikt. Der Einstieg in den Konflikt ist dadurch gegeben, dass mindestens zwei Akteure ihre Interessen darlegen und sich zeigt, dass sie einander entgegenstehen und die Akteure auf die Durchsetzung ihrer Interessen bestehen. In einem unkontrollierten Konflikt kann dieser an sich harmlose Informationsaustausch auf sehr unterschiedliche Art und Weise eskalieren. Der in der Abbildung gezeigte Kurvenverlauf ist also nicht zwingend und kann von Fall zu Fall anders aussehen. Soll der Konflikt überwunden werden, folgt auf die Eskalation des Konflikts eine Phase der Deeskalation, die schließlich mit einer Lösung endet. In unkontrollierten Konflikten ist es durchaus denkbar, dass ein zeitweise abgeflauter Konflikt, erneut aufflammt und sich

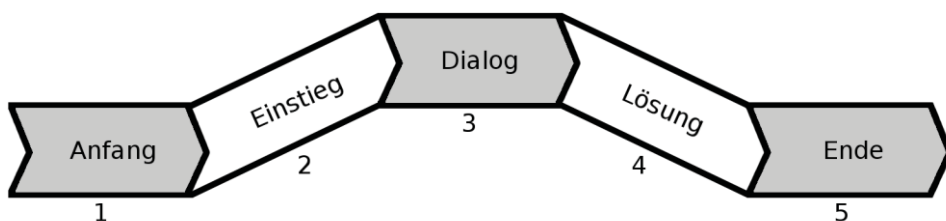
schlimmstenfalls dauerhaft hinzieht. Sie haben sicherlich von teilweise jahrzehntelang dauernden Nachbarschaftsstreitigkeiten gehört, die auch durch Gerichtsbeschlüsse nicht beizulegen sind.

Sicherheitsexperten sollten sich von der Hoffnung trennen, ohne Konflikte auszukommen: Sicherheitsmaßnahmen haben leider keinen Selbstzweck. Daher wird deren Umsetzung immer im Konflikt mit dem Ziel stehen, auf sie zu verzichten. Alle Konfliktanteile, die ein gewisses Maß übersteigen und eine unnötige Eskalation beinhalten, müssen umschifft werden. Es empfiehlt sich nach dem folgenden idealtypischen Ablauf vorzugehen:

1. Anfang
2. Einstieg in das Gespräch (Information)
3. Dialog (Argumentation)
4. Lösungssuche (Beschluss)
5. Beendigung

Nicht jedes Problem lässt sich mit nur einem Gespräch klären. Dann muss die Lösungssuche vertagt werden, auch wenn es schwer fällt. Es muss in jedem Fall vermieden werden, dass vorschnelle Lösungen auf den Tisch kommen, die nicht von allen Gesprächsteilnehmern mitgetragen werden. Das beendet zwar meist das Gespräch, nicht jedoch den Konflikt. Halbherzig akzeptierte Lösungen werden bald wieder in Frage gestellt.

Ein Gespräch ohne Lösung des Problems zu beenden, ist schwer zu ertragen – insbesondere für Führungskräfte und Entscheider. Daher ist es wichtig schwierige Gespräche nur dann zu beginnen, wenn man damit Aussicht auf Erfolg hat.



**Abbildung 3-8:** Die Konfliktpipeline<sup>58</sup>

<sup>58</sup> In Anlehnung an Karl Benien; Schwierige Gespräche führen; 2007; rororo; ISBN 9783499614774; Seite 124 ff

Im Folgenden wird der idealtypische Ablauf eines Gesprächs mit Hilfe der Konfliktpipeline in geregelte Bahnen geleitet. Die Konfliktpipeline ist in fünf Abschnitte eingeteilt, die den Konflikt parallel der unvermeidbaren Konfliktanteile aus Abbildung 3-7 entlang leitet.



**Abbildung 3-9:** Abschnitt 1: Der Anfang

Im 1. Streckenabschnitt geht es darum, die Gesprächspartner auf das Gespräch innerlich und äußerlich vorzubereiten. Dazu muss neben dem eigentlichen Gesprächsthema der äußere Rahmen geklärt werden. Woher kommen die Gesprächspartner? Haben sie gerade ein anstrengendes Meeting hinter sich? Wenn sich Ihr Gesprächspartner gerade eben über die IT-Abteilung geärgert hat ist es sicher keine gute Idee mit ihm über zusätzliche Einschränkungen durch Sicherheitsmaßnahmen zu sprechen, bevor nicht der Ärger über die IT-ler aus dem Kopf ist.

Wichtig ist in diesem Abschnitt auch, einen angenehmen Gesprächsrahmen zu schaffen. Das gilt zum einen äußerlich – also keine Störungen durch Telefon, E-Mail o.ä. – und zum andern innerlich. Unter Umständen müssen sie dazu gemeinsam gegen die IT-Abteilung wettern: *„Wirklich schlimm, wenn die Server immer dann ausfallen, wenn man sie am nötigsten braucht. Ich kann Ihren Ärger sehr gut verstehen. Da könnte man einiges in Sachen Ausfallsicherheit verbessern.“* In keinem Fall sollten sie ein Streitgespräch darüber eingehen, ob der Ärger überhaupt gerechtfertigt ist: Auf diesem Weg eskaliert das Gespräch, noch bevor das Thema Sicherheit überhaupt im Raum steht.

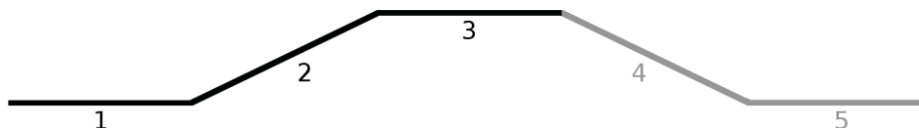
Wenn schon vor dem Gespräch feststeht, dass es um ein strittiges Thema geht, sollten sie einen gezwungenen Smalltalk über das Wetter oder das Wohlbefinden der Kinder lieber unterlassen, da diese netten Fragen schnell als unehrlich verstanden werden könnten, wenn Sie danach den Schwenk zum eigentlichen Streitpunkt machen.



**Abbildung 3-10:** Abschnitt 2: Der Einstieg

Im 2. Abschnitt der Konfliktpipeline müssen die Gesprächspartner ihren Standpunkt verdeutlichen, ohne jedoch schon in die Diskussion einzusteigen. Das beinhaltet, sich verständlich zu äußern und genau zuzuhören. Für IT-Sicherheitsbeauftragte, Datenschützer und Co. ist das Zuhören allerdings gar nicht so einfach. Ihre Gesprächspartner bringen in den seltensten Fällen das Fachwissen mit, eine konstruktive Aussage zu formulieren. Hier ist gezieltes Nachfragen nötig, ohne dabei schon zu bewerten, ob etwas geht oder nicht. Sie müssen Ihr Gegenüber also dabei unterstützen sich verständlich auszudrücken. Vielleicht fragen Sie sich jetzt: *„Warum soll ich denn dem anderen auch noch dabei helfen, seine verbohrt, technisch unmöglichen und viel zu teuren Vorstellungen zu äußern?“* Da es in diesem Abschnitt noch nicht darum geht die gemachten Aussagen zu diskutieren, liegt es in ihrem eigenen Interesse, diese *verbohrt, technisch unmöglichen und viel zu teuren Vorstellungen* genau zu verstehen – dieses Wissen wird ihnen im 3. Abschnitt der Konfliktpipeline zugutekommen.

Bleibt noch die Frage: *„Wer fängt an?“* Den Einstieg ins Thema sollten die Sicherheitsexperten suchen. Wenn sie dem Gesprächspartner den Vortritt lassen, wird dieser leicht unsicher und misstrauisch, weil die meisten Menschen instinktiv wissen, dass sie Gefahren nicht richtig einschätzen können. Wenn die Sicherheitsexperten den thematischen Einstieg übernehmen, vermeiden sie in jedem Fall, dass die Aussage ihres Gegenübers zu sehr daneben liegt.



**Abbildung 3-11:** Abschnitt 3: Der Dialog

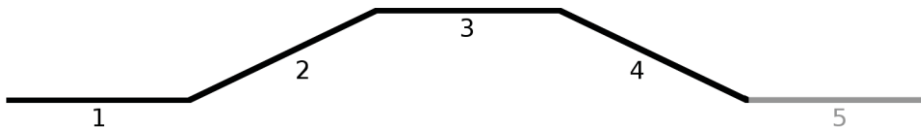
Die bisherigen Abschnitte der Konfliktpipeline waren nicht sonderlich schwer. Im 3. Abschnitt muss sie jedoch besonders stabil gebaut sein. Während im zweiten Abschnitt der Gesprächsdruck gestiegen ist, indem die Standpunkte ausgetauscht wurden, muss im dritten Abschnitt verhindert werden, dass sie mit immer eindringlicheren Worten bekräftigt oder endlos wiederholt werden. In Abbildung 3-7 waren das die grau hinterlegten unnötigen Konfliktanteile.

Am besten startet man in den dritten Abschnitt mit dem Beispielsatz über die konstruktive Kommunikation von Seite 66: *„Wir haben ein gemeinsames Problem, weil wir zur Zeit keine Idee haben, wie wir unsere gegensätzlich erscheinenden Ziele weitgehend vereinen können. Wir werden jedoch einen Weg suchen, das zu erreichen.“* Diese Aussage beinhaltet die einzuschlagende Richtung für die Dialogphase. In diesem Teil des Gesprächs werden die Argumente ausgetauscht, nachdem vorher klar umrissen wurde, was der Konfliktgegenstand ist. Es reicht nicht aus, jeweils im Wechsel die

eigene Position zu untermauern. Das würde nur der mittleren Ebene konstruktiver Kommunikation entsprechen: Man kennt und akzeptiert zwar die Meinung des Gesprächspartners, ist aber nicht bereit nach einem gemeinsamen Weg zu suchen.

Im Dialog müssen sich die Gesprächspartner einander annähern, ohne ihre eigenen Ziele aufgeben zu müssen. Im Grunde ist das nichts anderes, als auf dem Wochenmarkt um den Preis für ein Kilo Äpfel zu feilschen. Der Händler nennt einen Betrag und Sie nennen natürlich einen viel niedrigeren. Wenn Sie sich immer wieder wechselseitig die beiden Beträge aufsagen, kommen sie nicht weiter. Vielleicht will der Händler einfach einen bestimmten Gewinn mit dem Handel machen. Er schlägt Ihnen also vor, zwei Kilo Äpfel zu kaufen. Dafür kommt er Ihnen beim Kilopreis entgegen. Weil Ihnen das noch nicht reicht, sagen Sie, er müsse noch zwei Paprika obendrauf legen. Weil die Paprika ohnehin nicht mehr ganz so frisch sind, gibt der Händler wieder ein Stück nach usw.

Der Dialog findet also immer wechselseitig statt. Jeder ist dazu angehalten die Aussagen des anderen mit einfließen zu lassen. Ist Ihr Gesprächspartner dazu nicht bereit, müssen Sie diesen Part mit übernehmen – ähnlich wie schon im 2. Abschnitt der Konfliktpipeline. Wenn der Händler also auf seinem Preis beharrt, könnten Sie ihm vorschlagen, dass Sie zwei Kilo kaufen würden, wenn er im Preis nachgibt usw. Hier zahlt sich aus, ob Sie Ihrem Gegenüber im 2. Abschnitt richtig zugehört haben. Nur wenn Sie den Standpunkt Ihres Gesprächspartners kennen, können Sie jetzt gut verhandeln. Je genauer er sich zu Beginn inhaltlich festlegen musste, je weniger kann er Ihnen jetzt ausweichen.



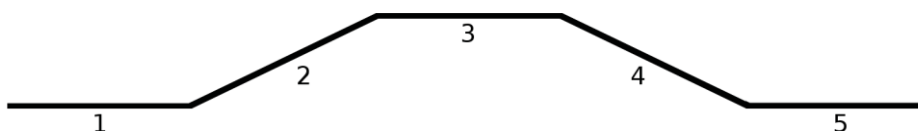
**Abbildung 3-12:** Abschnitt 4: Die Lösung

Dialogphase (3.) und Lösungsphase (4.) sind nicht immer klar voneinander zu trennen. Umso verlockender kann es sein, zu einer schnellen Lösung zu kommen. Dabei besteht die Gefahr, dass die Beteiligten mit der übereilten Lösung im Nachhinein doch nicht so zufrieden sind, wie anfänglich angenommen. Deshalb müssen im 4. Abschnitt der Pipeline die bisherigen Ergebnisse verdichtet und rekapituliert werden, so dass jedem noch einmal vor Augen geführt wird, was die Lösung genau beinhaltet.

Als Beispiel möchte ich kurz ein Erlebnis schildern, dass mir an einem Oliven-Stand passiert ist. Dort gab es viele tolle, in Öl eingelegte Sachen, die man mit Brot nach Herzenslust probieren konnte. Anfangs wollte ich nur ein Schälchen Oliven. Mit jedem Probierhappen kam jedoch ein weiteres Schälchen hinzu. Ich ging bester

Laune nach Hause. Die Qualität war wirklich toll. Leider musste ich die Hälfte wegwerfen, weil die Sachen nicht lange genug haltbar waren. Das Ganze hat mich nachträglich so geärgert, dass ich nie mehr an dem Stand eingekauft habe. Hätte mich der Verkäufer am Ende des Handels nochmal gefragt, ob ich das überhaupt alles essen kann, wäre ich sicher ein zufriedener Kunde geworden und wiedergekommen. Immerhin hatte ich zu Beginn gesagt, dass ich nur eine Schale Oliven will.

Auch wenn die Verlockung noch so groß ist, darf diese Phase nicht vernachlässigt werden. Ihr kommt eine ungeheure psychologische Bedeutung zu. Der unterdrückte Wunsch von heute ist der Vorwurf von morgen. Denken Sie an den Oliven-Stand.



**Abbildung 3-13:** Abschnitt 5: Das Ende

Im 5. Und letzten Abschnitt der Konfliktpipeline geht es darum, das Gespräch abzurunden. Gibt es noch offene „Reste“ oder Impulse für andere Gespräche? Bei größeren Sachverhalten kann hier das weitere Vorgehen vereinbart werden. Wenn es sich um besonders strittige Themen gehandelt hat, kann man hier besprechen, wie man das Gespräch empfunden hat und ob es weiteres Verbesserungspotential gibt.

### 3.3.1 Fallbeispiel: Unbegleitete Besuchergruppen

In dem Pharma-Unternehmen ExAmple AG ist Dave als Sicherheitsbeauftragter für die Sicherheit des Werksgeländes verantwortlich. Auf dem Werksgelände gibt es mehrere hochsensible Bereiche. Dazu gehören auch die chemischen Labore, die oft von Besuchergruppen aus Universitäten, der Lokalpolitik o.ä. besichtigt werden. Der Laborleiter Oskar macht die Führungen mit den Gruppen und muss sie im Anschluss zum Werkstor begleiten. In der Vergangenheit kam es vor, dass Dave Besuchergruppen ohne Begleitung auf dem Werksgelände angetroffen hatte. Dave hatte danach mit Oskar gesprochen, der sich schnell einsichtig zeigte. Nach einigen Wochen wiederholte sich der Vorfall. Auch da sah Oskar seinen Fehler schnell ein und gelobte Besserung. Wieder einige Wochen später traf Dave sogar auf dem Flur des Labortrakts auf eine unbegleitete Besuchergruppe und ist darüber nun ziemlich verärgert.

Wie könnte Dave das dritte Gespräch angehen, wenn er ohnehin erwarten muss wieder nur leere Versprechungen zu bekommen? Eigentlich möchte er am liebsten an die Decke gehen. Entlang der fünf Abschnitte der Konfliktpipeline kann Dave seine Energie kanalisieren. Zum Einstieg sollte Dave direkt zur Sprache bringen, um was es ihm geht. Lange um den heißen Brei reden, bringt hier wenig. Nachdem Dave dafür gesorgt hat, dass das Gespräch nicht unnötig gestört wird, steigt er direkt ins Thema ein:

*„Oskar, wir treffen uns hier zum dritten Mal, weil Sie eine Besuchergruppe nicht wie vorgesehen zum Werkstor eskortiert haben. Zuletzt habe ich eine Gruppe sogar im Laborbereich angetroffen. In den beiden Gesprächen zuvor haben Sie jeweils eingesehen, dass das nicht nur gegen unsere Richtlinien verstößt sondern auch gefährlich ist und versprochen, dass es nicht wieder vorkommt. Ich möchte heute mit Ihnen darüber sprechen, warum Sie ihr Versprechen nicht gehalten haben. Mein Ziel ist es mit Ihnen eine Vereinbarung zu treffen, die nicht wieder gebrochen wird.“*

Damit wäre der Anfang gemacht – klar, treffend, knapp und wertfrei. In den Abschnitten 2 und 3 müssen nun die Argumente ausgetauscht werden. Für Dave ist besonders wichtig, herauszubekommen, was Oskars Ziel ist. Sein Ziel ist ja sicher nicht, zwei Mal im Monat eine Besuchergruppe „laufen zu lassen“. Dave erreicht das durch gezieltes Nachfragen. Gerne würde Oskar einfach wieder versprechen, dass es nicht wieder vorkommt. Diesmal lässt Dave aber nicht locker und widersteht der Versuchung einer schnellen Problemlösung. Nach einigem hin und her sagt Oskar, dass der Chef ihn manchmal direkt aus den Besucherführungen reißt und er dann keine Zeit mehr hat, sie nach draußen zu eskortieren. Da er nicht unhöflich sein wolle, würde er sie bitten, ohne ihn das Gelände zu verlassen:

*„Ich kann doch den Herrn Professor oder den Bürgermeister nicht im Laufschrift zum Tor rauswerfen – das mach’ ich nicht! Kann der Alte wegen mir selber machen!“*

Dave ist durch sein gezieltes Nachfragen auf den Kern des Problems gestoßen. Jetzt gilt es mit Oskar eine Lösung zu erarbeiten, die ihm aus seinem Dilemma heraushilft. Im letzten Abschnitt der Konfliktpipeline sollten die beiden vereinbaren in Zukunft früher über solche Probleme zu sprechen, bevor die Sicherheit gefährdet wird. Für solche Probleme ist Dave doch da.

### 3.4 Motivation

Ohne Motivation geht nichts. Motivation ist ein Schlüsselthema, wenn man Konflikte vermeiden möchte. Wie kann man jemanden dazu bringen, zu tun, was man von ihm will? Diese Frage beschäftigt die Motivationspsychologie seit Jahrzehnten, ohne dabei auf den Stein der Weisen gestoßen zu sein.



**Abbildung 3-14:** Wie man richtig motiviert ist nicht so einfach, wie man denkt.

Zunächst wäre da die Möglichkeit den Mitarbeiter zu bitten. Aber was, wenn der keine Lust hat und sich von freundlichen Bitten nicht beeinflussen lässt? Kommt man dann mit strammen Anordnungen weiter? Möglicherweise, wenn es darum geht eine bestimmte Aufgabe zu erledigen. Wenn es aber darum geht jemanden dauerhaft dazu zu bringen, sich auch ohne Aufsicht an Sicherheitsmaßnahmen zu halten, führt das auch nicht zwangsläufig zum Erfolg. Sollte also Geld ein möglicher Anreiz sein, sich an Sicherheitsrichtlinien zu halten? Jede verschlüsselte Mail bringt 10 Cent, jede unverschlüsselte kostet diesen Betrag? Wenn man erreichen will, dass sich die Mitarbeiter verschlüsselte Mails mit sinnlosem Inhalt zuschicken, könnte das helfen. Oder kommt man etwa mit militärischem Starrsinn zum Ziel: Vormachen, Nachmachen und drillmäßiges Üben?<sup>59</sup> Sicher kann ein ausgefeiltes Training der Schlüssel zum Erfolg sein. Alle Mitarbeiter erreicht man so aber auch nicht. Oder sollte man den Mitarbeitern hier und da einen Schubs in

<sup>59</sup> Frederick Herzberg; Was Mitarbeiter in Schwung bringt, in: Motivation: Was Manager und Mitarbeiter antreibt; 2006; Redline Wirtschaft; ISBN: 9783636014078; Seite 71 ff 

die richtige Richtung geben, in der Art wie der Signalton im Auto, der einen erinnert, das Licht angelassen zu haben? Das funktioniert jedoch nur bei Dingen, an die man auch erinnert werden möchte. Wenn alles versagt, kann man nötigenfalls durch Angst motivieren: *"Sicherheitsvorschriften einhalten, sonst Kündigung!"* Aber auch das ist zum Scheitern verurteilt, wenn die Geschäfts- oder Behördenleitung nicht motiviert ist. Wie motiviert man den Chef? Man kann dem eigenen Chef ja schlecht mehr Gehalt versprechen.

Nicht alles, was dazu geeignet ist Mitarbeiter, Manager und Chefs im Allgemeinen zu motivieren, eignet sich auch dazu sie für Sicherheitsfragen zu begeistern. Außerdem ist es im Allgemeinen vielleicht ein Erfolg, wenn ein Mitarbeiter an 95% aller Arbeitstage voll motiviert ist und die restlichen 5% etwas nachlässt. In Sicherheitsfragen reicht das aber nicht: Wenn der Wachmann aus Nachlässigkeit in 5% der Nächte die Alarmanlage nicht aktiviert, stehen den Einbrechern immerhin an 18 Tagen im Jahr die Türen offen. Das kann man beim besten Willen nicht als Erfolg bezeichnen. Es ist auch kein Erfolg, wenn 95% der vertraulichen Mails verschlüsselt werden oder „nur“ 5% der Kreditkartendaten aus dem Webshop abhandenkommen. Sicherheitsexperten stehen vor keiner geringeren Aufgabe als alle Beteiligten zu 100% zu motivieren. Ob auf einer Baustelle ein Handwerker schläft oder zwanzig ist ein großer Unterschied, und es wäre ein Erfolg, wenn man erreichen würde, dass nur noch einer schlief und alle anderen arbeiten. Für Sicherheitsexperten ist es aber leider egal, ob die Konkurrenz die brandneue Entwicklung von einem oder von zwanzig Mitarbeitern zugespielt bekommt.

Wer sich einer solchen Herausforderung stellen soll, muss nicht zuletzt sich selbst immer wieder aufs Neue motivieren, scheint das gesteckte Ziel doch kaum zu erreichen und vieles vom Zufall abzuhängen. Zum Beispiel, dass die Einbrecher hoffentlich an einem Tag vor der Tür stehen, an dem die Alarmanlage aktiviert ist.

### 3.4.1 Was ist Motivation

Bevor die Frage, was Motivation ist, in Form einer Definition beantwortet wird, soll klar gemacht werden, was sie nicht ist: Motivation ist deutlich von der Manipulation abzugrenzen. Suggestivfragen, Polemik oder Demagogie gehören zu den manipulativen Methoden, die vielleicht zum Ziel führen, denen jedoch eine klare Absage zu erteilen ist.<sup>60</sup> Manipulation schadet jeder Bemühung ein Vertrauensverhältnis aufzubauen und damit auch dem Versuch konfliktpräventiv

---

<sup>60</sup> William P. Ferris in: Norbert Albs; Wie man Mitarbeiter motiviert: Motivation und Motivationsförderung im Führungsalltag; 2005; Cornelsen Verlag Scriptor; ISBN: 9783589236800; Seite 14 ff ➡

zu kommunizieren. *Manipulation* zeichnet sich u.a. durch die folgenden negativen Eigenarten aus:

- ✗ Verschleierung von Tatsachen zum eigenen Vorteil
- ✗ Einseitige Begrenzung von Informationen oder Kontakten
- ✗ Unbewiesene oder unwahre Behauptungen

Demgegenüber sind die Eigenarten<sup>61</sup> des *Motivierens* durchweg mit einer positiven Ausrichtung auf die zu motivierende Person ausgerichtet:

- ✓ Jemanden mit Motiven ausstatten, die dieser vorher nicht hatte
- ✓ Vorhandenen Motiven zur Realisierung verhelfen
- ✓ Verhaltensweisen eine (subjektive) Bedeutung verleihen
- ✓ Anregen, begeistern, gewinnen

Wer motiviert, nimmt Einfluss auf Inhalt, Richtung, Intensität des Handelns einer anderen Person, ohne sie dabei zu manipulieren. Auch hier erkennt man sofort, welche Bedeutung eine ausgeprägte Motivationsstärke für IT-Sicherheitsbeauftragte, Datenschützer und Co. hat. Dreht sich doch deren Aufgabe in weiten Abschnitten um nichts anderes, als menschliches Handeln und Unterlassen zu beeinflussen.

Aus psychologischer Sicht unterscheidet man Motivation nach den zwei Formen intrinsischer und extrinsischer Motivation. Für Sicherheitsexperten gilt die Faustregel: Andere extrinsisch und intrinsisch motivieren, sich selbst intrinsisch. Selten hört man von IT-Sicherheitsbeauftragten, die auch noch dazu angestachelt werden, die Rechtevergabe auf dem Server noch restriktiver umzusetzen und ebenso selten sind die Berichte über Mitarbeiter, die das Datenschutzkonzept besser kennen als der Datenschutzbeauftragte, weil sie einfach von sich aus Interesse am Schutz personenbezogener Daten haben. Es sei denn, es betrifft die eigene Person. Unter Umständen entfaltet sich dann doch ein Maß an intrinsischer Motivation, das durch Einflussnahme von außen nie zu erreichen gewesen wäre.

Wer Mitarbeiter, Chefs und letztlich sich selbst motivieren will, der muss sich an die vier Problemfelder aus Kapitel 1 erinnern: Ziele, Zwänge, Prioritäten und Risiken. Aus ihnen lassen sich die Motivatoren und Hygienefaktoren ableiten, auf deren Grundlage man zu einer Verhaltensänderung motivieren kann. *Motivatoren* sind nach vorne gerichtet. Sie sind bestimmend für die Zufriedenheit und motivieren zu Leistung und gegebenenfalls zur Leistungssteigerung. Die

---

<sup>61</sup> Reinhard K. Sprenger, Thomas Plassmann; *Mythos Motivation: Wege aus einer Sackgasse*; 2005; Campus Verlag; ISBN: 9783593376370; Seite 21 

*Hygienefaktoren* haben zwar nicht diese motivierende Kraft. Bei ihrem Fehlen jedoch sorgen sie für Demotivation und Unzufriedenheit. Motivatoren erzeugen überwiegend intrinsische Motivation, wohingegen Hygienefaktoren eher extrinsisch motivieren. Herzberg hat diesen Zusammenhang in seiner Zwei-Faktoren-Theorie beschrieben.<sup>62</sup>

| <b>Motivatoren</b><br>Führt zu Zufriedenheit | <b>Hygienefaktoren</b><br>Führt zu Unzufriedenheit |
|----------------------------------------------|----------------------------------------------------|
| Erfolg                                       | Unternehmens-Organisation                          |
| Anerkennung                                  | Dienstaufsicht                                     |
| Arbeitsinhalt                                | Verhältnis zu Vorgesetzten                         |
| Verantwortung                                | Arbeitsbedingungen                                 |
| Vorwärtskommen                               | Bezahlung                                          |
| Entwicklung                                  | Verhältnis zu Kollegen/ Mitarbeitern               |

**Tabelle 3-3:** Motivatoren und Hygienefaktoren nach F. Herzberg

In Tabelle 3-3 sind einige Motivatoren und Hygienefaktoren aufgelistet. Die wichtigsten stehen in der Tabelle jeweils oben. Grundlage dieser Einordnung waren 12 Mitarbeiterbefragungen, bei denen über 3500 Vorfälle am Arbeitsplatz erfasst wurden. Die genannten Begriffe wurden von den Befragten auf die eine oder andere Seite der Tabelle „gewählt“. Im Individuellen Fall kann beispielsweise der Arbeitsinhalt durchaus als Hygienefaktor empfunden werden, oder die Bezahlung als Motivator. Man erkennt jedoch auf den ersten Blick, dass Sicherheitskonzepte, Sicherheitsaudits und Sicherheitsrichtlinien allesamt auf der rechten Seite der Tabelle beheimatet sind und überwiegend dazu geeignet sind Unzufriedenheit zu erzeugen. Es scheint also angebracht und am vielversprechendsten, Sicherheitsanstrengungen mehr in Richtung der Spalte mit den Motivatoren zu verlagern, wenn man unnötige Konflikte vermeiden will. Die im Folgenden vorgestellten Ansatzpunkte werden sich an diesem Ziel orientieren und damit einen weiteren Baustein liefern, der es Sicherheitsexperten ermöglicht, der „Buhmann-Falle“ zu entkommen.

<sup>62</sup> Nach F. Herzberg in Norbert Albs; Wie man Mitarbeiter motiviert: Motivation und Motivationsförderung im Führungsalltag; 2005; Cornelsen Verlag Scriptor; ISBN: 9783589236800; Seite 71 ff 

### 3.4.2 Motivation von Geschäfts- und Behördenleitung

Die wahrscheinlich schwierigste Motivationsaufgabe für Sicherheitsexperten ist es, diejenigen zu überzeugen, die für die Sicherheit im Unternehmen verantwortlich sind: Die Chefs. Nur sind die sich dieser Verantwortung meist nicht bewusst. Oft stößt man bei Geschäfts- und Behördenleitung auf die Ansicht, dass sie durch die Anstellung von IT-Sicherheitsbeauftragten, Datenschutzern und Co. die Verantwortung loswerden. Den Sicherheitsexperten kommt das vielfach gelegen, wurde doch gerade verdeutlicht, dass Verantwortung ein starker Motivator ist. Wer Chefs motivieren will muss ihnen diese Verantwortung – ganz selbstlos – zurückgeben, auch wenn das negative Auswirkungen auf die eigene Motivation haben könnte.



**Abbildung 3-15:** Malen Sie dem Chef ruhig mal den Teufel an die Wand

Anerkennung ist ein weiterer Motivator, der einen Blick wert ist. Wenn der Chef sich also neben all den Problemfeldern als Unternehmens- oder Behördenleiter für die Security-Bühne interessiert, dann kann man das gar nicht genug loben. Das soll natürlich nicht heißen, dass Sie jeden Tag zum Chef sollen, um ihm mitzuteilen wie toll er ist – Anerkennung nach oben darf nicht zur Speichelleckerei verkommen. Die Anerkennung, die Sicherheitsexperten zu vergeben haben, ist eine fachliche. In der Kombination mit dem Motivator Verantwortung bedeutet das: Malen Sie dem Chef ruhig mal den Teufel an die Wand und zeigen ihm auf, wie groß die Verantwortung ist, die er trägt und loben Sie sein Verständnis für die schwer zu verstehenden Zusammenhänge von Bedrohung, Gefahr und Sicherheit.

Je nach Typ kann auch Arbeitsinhalt ein vielversprechender Motivator für Chefs sein. Chefs müssen ihren Interessen entsprechend in die Arbeitsprozesse eingebunden werden. Der Verwaltungstyp will organisatorisch eingebunden werden, der Techniker lieber in die kleinen Spielereien, die vielleicht auch zuhause zu gebrauchen sind. Dabei ist vor allem nötig, die eigenen Problemfelder in die der Chefs zu übersetzen und sie für Sicherheit im Allgemeinen zu begeistern – der Rest kommt dann fast von selbst. Um den folgenden Beispielen ein wenig vorwegzugreifen: Für den Verwaltungstyp ist der Live-Hacking-Event vor allem von seiner organisatorisch, rechtlichen Seite interessant, während man den technikbegeisterte Chef am besten die Rolle des Hackers übernehmen lässt, der die Befehle für die Man-In-The-Middle-Attacke mittels ARP-Spoofing eintippt und abends dem Junior erzählen kann, dass er ein Hacker ist.

Es lohnt sich darüberhinaus, die Motivatoren persönliche Entwicklung und Erfolg anzusprechen, insbesondere in einer globalisierten Wissens- und Kommunikationsgesellschaft. Wer als Chef auch in fünf oder zehn Jahren noch mithalten will, muss sich mit dem Wachstumsmarkt Sicherheit auseinandersetzen. Ein routiniertes Standing in einer globalisierten und vernetzten Welt ist für Entscheider ein wichtiger Erfolgsfaktor. Was sich nach allen gängigen Theorien zur Motivationspsychologie in keinem Fall lohnt, sind Anstrengungen, die die Hygienefaktoren betreffen. Kein Chef dieser Welt lässt sich für Sicherheit begeistern, weil er sich dann mit dem Sicherheitsteam besser versteht.

*„Gebranntes Kind scheut das Feuer“*, sagt der Volksmund und drückt damit aus, dass es eine Sache ist, von einer Gefahr zu wissen, und eine andere, eine Gefahr gespürt zu haben. Was das Sprichwort beschreibt, lässt sich auch an konkreten Zahlen festmachen. In einer Studie zur Wirtschaftskriminalität 2009 gaben die Befragten aus Unternehmen, die bereits Opfer von Datendiebstählen wurden, eine erheblich höhere Risikoeinschätzung für sich und andere Unternehmen ab: Während in nicht geschädigten Unternehmen nur 10% das Risiko für das eigene Unternehmen als hoch einschätzen, sahen das in geschädigten Unternehmen hingegen 34% der Befragten so – mehr als drei Mal so viele.<sup>63</sup> Und das, obwohl davon auszugehen ist, dass in den betroffenen Unternehmen Maßnahmen gegen eine Wiederholung der Vorfälle getroffen wurden. Auch wenn Vorfälle deutliche Auswirkungen auf die Risikoeinschätzung haben, wird man sie sich doch nicht herbeiwünschen.

Die Frage lautet also, wie man dem Kind das Feuer möglichst anschaulich macht, ohne das es dabei Verletzungen davon trägt. Ein kleiner Schreck ist dabei durchaus erlaubt: Zwei mögliche Ansätze sind Live-Hackings und Penetrations-Tests.

---

<sup>63</sup> Martin-Luther-Universität Wittenberg und PricewaterhouseCoopers; Wirtschaftskriminalität 2009: Sicherheitslage in deutschen Großunternehmen; 2009; Bezug über: [www.pwc.de/de/crimesurvey](http://www.pwc.de/de/crimesurvey); Seite 34

### 3.4.2.1 Live-Vorfürhrungen/ Live-Hacking

Bei Live-Vorfürhrungen geht es darum, zu erläutern, wie einfach, schnell und effektiv ein Unternehmen aus den Angeln gehoben werden kann, wenn es sich nur ausreichend verwundbar zeigt. Am Ende der Vorfürhrung müssen alle Zuschauer sagen: „*Oh Gott, so einfach geht das?!*“ Die Angriffe werden dabei in Testsystemen vorgeführt, und sind relativ einfach vorzubereiten und einzustudieren. Mit der Auswahl eines passenden Szenarios lassen sich die Ergebnisse in die gewünschte Richtung lenken und verschiedene Aspekte der Sicherheitsarchitektur ansprechen. Einige der folgenden Szenarien sind den Webseiten des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen entnommen, auf denen sich auch Videos einzelner Vorfürhrungen finden.

Die Auswahl geeigneter Szenarien hängt allerdings nicht nur am verfolgten Ziel, sondern auch an den nötigen fachlichen Kenntnissen. Nicht für jeden ist es empfehlenswert einen Versuchsaufbau mit einem trojanischen Pferd vorzubereiten, oder den Infektionsweg mit einem Virus darzustellen. Man sollte sich auf eine solche Vorfürhrung nur einlassen, wenn man wirklich weiß, was man tut, und das innerhalb des Unternehmens oder der Behörde entsprechend abgestimmt hat. Im Zweifel sollte man sich externe Unterstützung holen: Die Auswahl an Unternehmen, die Live-Hackings für Schulungen anbieten ist reichhaltig.

Mit ein wenig Übung kann man auch mit begrenzten Mitteln und ohne große technische Kenntnisse ansehnliche Vorfürhrungen gestalten, die zum gewünschten Erfolg führen. Im Folgenden sollen nun einige weniger schwierige Möglichkeiten vorgestellt werden.

**Google-Hacking:** Beginnen wir mit einem ganz leichten Beispiel: In Google sehen die meisten Menschen eine mächtige Suchmaschine: Zwei, drei Wörter in die Suchzeile und schon bekommt man die gewünschten Resultate. Dass Google auch Angreifer mit einer geradezu unglaublichen Fülle von Informationen versorgt, ist nicht jedem bekannt und Bücher wie *Google Hacking*<sup>64</sup> von Johnny Long haben hauptsächlich die IT-Welt erreicht. Seine Google Hacking Database (GHDB) ist frei im Internet zu erreichen.<sup>65</sup> Hier finden sich hunderte von Google-Suchanfragen, mit deren Hilfe Angriffe eingeleitet werden können. Das Besondere: Sie müssen die Suchen nicht einmal selber eintippen – einfach anklicken und die

---

<sup>64</sup> Johnny Long; *Google Hacking*; 2005; Mitp; ISBN: 9783826615788

<sup>65</sup> <http://johnny.ihackstuff.com/ghdb/>

Suchergebnisse auswerten. Mit der Anfrage `intitle:"Index of" Buchhaltung.xls` liefert Google alle Excel-Tabellen mit diesem Namen, die im Internet zu finden sind – fast alle sind aus Versehen auf irgendeinem Webserver gelandet. Mit ein paar Klicks und ein wenig Fantasie lassen sich auf diese Art tolle Beispiele finden.

**Geschwärzter Text:** Ebenso einfach können Sie vorführen, wie schnell man mit PDF-Dateien auf die Nase fallen kann. Alles was sie tun müssen ist, einen einigermaßen bekannt gewordenen Fall nachzustellen, bei dem das Pentagon keine gute Figur abgegeben hatte: Entscheidende Teile eines Dokumentes waren zwar zunächst in Microsoft Word geschwärzt, aber dann mit PDFMaker 6.0 exportiert worden. Dabei blieben die geschwärzten Textstellen erhalten und ließen sich über die Zwischenablage wieder herstellen.<sup>66</sup> Probieren Sie aus, ob der Fall mit Ihrer Software auch passiert wäre und führen Sie das Ergebnis vor.

**Metadaten:** Als weiteres Problem bei der Sicherheit von Dokumenten stellen sich immer wieder die Metadaten heraus. Mit Metadaten werden, meist in den Dokumenteigenschaften, zusätzlich weitere Informationen angegeben, wie beispielsweise der Autor oder das Erstellungsdatum. Stellen Sie sich vor, aus den Metadaten einer Marketing-Broschüre geht hervor, dass diese eigentlich bei der Konkurrenz abgekupfert ist. Der Chef wäre sicher begeistert, davon beim Sonntagsfrühstück in der Zeitung zu lesen.

**Wayback-Machine:** Hinter diesem Begriff<sup>67</sup> verbirgt sich ein Internet-Archiv, das Zwischenstände von Internet-Seiten speichert und dauerhaft archiviert. Unter Umständen entstehen daraus Datenschutzprobleme. Haben Sie zu allen Mitarbeiterfotos, die auf Ihren Webseiten veröffentlicht wurden jeweils eine Einverständniserklärung. Oder finden sich in diesen Archiven vielleicht peinliche Fehler, die auf den Seiten mal zu sehen waren? Mit ein wenig Recherche finden Sie tolle Beispiele zum Thema: „*Das Internet vergisst nichts.*“

---

<sup>66</sup> <http://www.heise.de/newsticker/meldung/Pentagon-blamiert-sich-mit-geschaerztem-PDF-Dokument-157946.html> eingesehen am 15.10.2009, archiviert unter: <http://www.webcitation.org/5kXe250t6>

<sup>67</sup> <http://www.archive.org>

**Tür-Falle:** Etwas mehr technisches Geschick erfordert eine Vorführung, bei der man zeigen kann, wie wichtig es ist, Türen zu sicherheitsempfindlichen Bereichen, die mit einem Türknauf statt einer Klinke ausgestattet sind, nicht nur zuzuziehen, sondern auch abzuschließen: Als Falle bezeichnet man den Schnapp-Mechanismus einer Tür, der in Krimis gerne mittels einer Kreditkarte ausgehebelt wird. Alles was man für einen „Einbruch“ benötigt, ist eine längliche Plastikkarte. Kreditkarten zerbrechen übrigens – das klappt nur im Film! Das Öffnen einer solchen Tür ist nach einiger Ausdauer beim Üben in wenigen Sekunden bis Minuten möglich – auch für Laien.

**Phishing:** Mit ein wenig Unterstützung vom Web-Administrator lässt sich vorführen, wie leicht man an Nutzernamen und Passwort gelangt: Mit einer Mail lockt man einen Anwender zu einer gefälschten Eingabemaske, die nach Nutzernamen und Passwort fragt, und aussieht, wie die echte Eingabemaske. Nach der ersten Eingabe des Passworts kommt die Fehlermeldung für ein falsches Passwort und die Originalseite wird aufgerufen. Dass auf diese Weise die Zugangsdaten gestohlen wurden, bleibt dem Anwender verborgen.

Wie Sie sehen, kann man auch mit begrenzten Mitteln und ohne selbst ein Hacker zu sein, über Live-Vorführungen nachdenken. Wenn Sie Glück haben macht sich bei Ihrem Chef während der Vorführung eine leise Panik breit, und er stellt am Ende entsetzt fest, auf welch wackligen Beinen die Sicherheit seines Unternehmens oder seiner Behörde steht. Wenn Sie mehr Möglichkeiten haben oder über mehr technisches Knowhow verfügen, dann können Sie auch fortgeschrittene Techniken einsetzen. Vergessen Sie dabei aber nicht, dass es sich bei derartigen Vorführungen immer um ein Spiel mit dem Feuer handelt. Es könnte sein, dass der Chef gar nicht begeistert davon ist, wenn der Sicherheitsbeauftragte vorführt, wie man ins Warenlager einbrechen kann, ohne dabei erwischt zu werden.

In Tabelle 3-4 sind die bisher genannten Beispiele zusammen mit weiteren Szenarien für Live-Vorführungen und Live-Hackings aufgeführt. Zu den meisten Szenarien finden Sie im Internet zahlreiche Videos, mit denen Sicherheits-Dienstleister für Ihre Vorführungen werben.

Eine Link-Liste finden Sie im OnlinePLUS-Service zu diesem Buch unter <http://www.viewegteubner.de/tu/Konfliktmanagement>.

| Bereich                            | Schwachstelle                               | Szenarien-Beispiel                                                                                                                                                                     |
|------------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Physikalische Sicherheit</b>    | Tür-Falle<br>Türschloss<br>Gekippte Fenster | Kreditkarten-Einbruch*<br>Schlüsseldienst einladen (Lock-Picking)<br>Schlüsseldienst einladen                                                                                          |
| <b>Datenschutz</b>                 | Telefon<br>Website<br>Mitarbeiter           | Frage-Anruf/ Social Engineering<br>Surfen mit der Wayback-Machine*<br>Personensuche im Internet                                                                                        |
| <b>Sicherheit der Plattform</b>    | Spaß-Software<br>USB                        | Trojaner vorführen<br>Autostart-Funktion ausnutzen                                                                                                                                     |
| <b>Sicherheit im Web</b>           | E-Mails<br>Webseite<br><br>Webserver        | Phishing E-Mail*<br>Cross Site Scripting (XSS)<br>ARP-Spoofing<br>Google-Hacking*                                                                                                      |
| <b>Sicherheit von Zugangsdaten</b> | Passwörter<br><br>Benutzernamen             | Datenbank-Angriff vorführen<br>Brute-Force-Angriff vorführen<br>Daten-Sammlung mittels Skript                                                                                          |
| <b>Mobile Sicherheit</b>           | Smartphone<br><br>Bluetooth<br><br>WLAN     | Handy-Trojaner vorführen<br>GPS-Ortungs-Software zeigen<br>Telefonbuch-Einträge ändern<br>Das Headset als Wanze benutzen<br>WEP-Verschlüsselung knacken<br>Wardriving-Stadtplan zeigen |
| <b>Sicherheit von Dokumenten</b>   | Passwortschutz<br>PDF                       | Word-Passwortschutz knacken<br>Unerwünschte Metadaten anzeigen*<br>Geschwärzten Text sichtbar machen*                                                                                  |

**Tabelle 3-4:** Mögliche Szenarien für Live-Vorführungen<sup>68</sup> (\* im Text bereits ausführlicher vorgestellt)

<sup>68</sup> Teilweise aus: Institut für Internet-Sicherheit; FH Gelsenkirchen; <http://www.internet-sicherheit.de/service/live-hacking-awareness-performance/szenarien/> eingesehen am 15.10.2009; archiviert unter <http://www.webcitation.org/5kXXHiAYH>

### 3.4.2.2 Penetrations-Tests

Während bei Live-Vorführungen nur theoretisch gezeigt wird, wie leicht ein Unternehmen angreifbar wäre, wird bei Penetrations-Tests (oder kurz: Pen-Tests) gezielt nach Schwachstellen gesucht und am Ende der Tests müssen die Verantwortlichen sagen: „*Das lief ja gut*“, oder – was wahrscheinlicher ist – „*So geht's nicht weiter!*“ Die Gefahr für das Unternehmen ist dabei weniger, dass Schwachstellen aufgedeckt werden, sondern mehr, dass die Verantwortlichen nicht ausreichend auf diese Missstände vorbereitet wurden und aus allen Wolken fallen. Die Angriffe werden im Gegensatz zu Live-Vorführungen nicht in Testsystemen durchgeführt. Die Operation wird quasi am offenen Herzen durchgeführt – mit entsprechend hohem Risiko. Will man also Konflikte vermeiden, muss ein Penetrations-Test umfangreich vorbereitet, begleitet und nachbereitet werden. Aber auch hier lassen sich mit der Auswahl von passenden Methoden die Ergebnisse in eine gewünschte Richtung lenken und verschiedene Aspekte der Sicherheitsarchitektur ansprechen.

Die Frage, ob man Pen-Tests selbst durchführt oder extern vergibt, stellt sich eigentlich nicht. Erstens sind verglichen mit Vorführungen viel tiefergehende Kenntnisse nötig, um ein aussagekräftiges Ergebnis zu erzielen; Pen-Tests lassen sich schwer einüben. Zweitens simulieren die Tests einen echten Angreifer – Neutralität bezüglich der Sicherheitsmaßnahmen ist also nötig. Befangene Pen-Tester würden das Ergebnis beeinflussen. Ein eigenes Team aufzustellen macht also nur Sinn, wenn das Unternehmen oder die Behörde, für die man arbeitet, groß genug sind, und diese Neutralität sichergestellt ist.

Ein weiterer Aspekt macht Pen-Tests schwieriger als Vorführungen: Es werden ja im Grunde strafbare Handlungen simuliert und das erfordert eine klare Aufgabenbeschreibung und fundierte juristische Beratung. Es reicht sicher nicht aus, dass der IT-Sicherheitsbeauftragte einem alten Studienfreund am Telefon beauftragt, zu probieren, wie weit er an der Firewall kommt. Es muss vorher genau festgelegt werden, welche Testmethode angewendet wird, und was genau getestet wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich in einer Studie mit dieser und anderen Fragestellungen zum Thema Pen-Tests auseinandergesetzt.<sup>69</sup>

Bevor wir uns die einzelnen Testmethoden genauer ansehen ist jedoch ein Blick auf das Konfliktpotential eines Pen-Tests angebracht. Während Vorführungen theoretisch zeigen, welche Auswirkungen schlecht konfigurierte Server und Netzwerke haben, werden hier ganz praktische Mängel offenbar, die irgendjemand zu verantworten hat. Möglicherweise zeigt sich sogar, dass jemand in der

---

<sup>69</sup> Bundesamt für Sicherheit in der Informationstechnik; "Durchführungskonzept für Penetrationstests"; 2003; Seite 18 

Vergangenheit sehr schlechte Arbeit gemacht hat. Will man im Anschluss an den Test nicht in ein Konflikt-Chaos stürzen, sollte man sich Gedanken über das Worst Case Szenario machen, durch das sich viele vor den Kopf gestoßen fühlen könnten. Angefangen bei Geschäfts- und Behördenleitung, über das IT-Personal, bis hin zu den Security-Experten: Für jeden kann ein Pen-Test ein Experiment mit offenem Ausgang sein.

Die größten Schwierigkeiten können entstehen, wenn sich die Chefs falschen Hoffnungen hingegen haben. Sie müssen sich auf ihre Fachleute verlassen. Auch wenn sie ihnen nicht die nötige Unterstützung gegeben haben, werden sie die Schuld für ein schlechtes Abschneiden wohl kaum bei sich selbst, sondern bei den Sicherheitsexperten suchen. Dieser Eindruck muss natürlich unter allen Umständen verhindert werden, sonst stehen IT-Sicherheitsbeauftragte, Datenschützer und Co. nach dem Test schlechter da wie vorher. Ebenso wenig sinnvoll ist es, vom schlimmsten Fall auszugehen, und dann passiert nichts. Wenn der Chef am Ende sagt, *„ist ja dann doch nicht alles so schlimm wie Sie immer sagen“*, haben Sie sich einen Bärenienst erwiesen. Das gute Ergebnis des Tests steht ihnen dann selbst im Weg. Was also ist der richtige Weg?

Den Chefs muss von Anfang an klar werden, dass es sich beim Testergebnis um eine Momentaufnahme eines kleinen Bereichs der gesamten Sicherheit handelt. Es werden nie alle möglichen Angriffsvektoren geprüft und es werden auch nie alle möglichen Bereiche des Unternehmens geprüft. Weder ein gutes, noch ein schlechtes Ergebnis lassen also eine Aussage zur Gesamtsicherheit zu – das muss den Beteiligten zuvor klar sein und in der Planungsphase berücksichtigt werden. Wenn das IT-Personal durch ein schlechtes Ergebnis aus dem Tiefschlaf gerissen wird, hat es sich die Suppe meist selbst eingebrockt – das ist einfacher. Trotzdem bleiben Frustration und das Gefühl, von den Initiatoren des Pen-Tests ans Messer geliefert worden zu sein.

Am besten ist es, wenn keiner der Beteiligten zu dem Test überredet werden musste, sondern ihn von sich aus gewollt hat. Dafür ist es wichtig, bei diesen vorher auf Tuchfühlung zu gehen und nicht gleich mit der Tür ins Haus zu fallen. Dass ein Pen-Test für die IT-Administratoren sonst wie die Aufkündigung des gegenseitigen Vertrauens aussieht, liegt auf der Hand. Eine gute Vorbereitung sind die im vorigen Abschnitt besprochenen Vorführungen, die das Eis brechen können. Hat der Administrator die Gefahr erst live vor Augen, ist er leichter bereit, auch eigene Fehler zu vermuten und ihnen auf den Grund zu gehen.

Der Ablauf eines Pen-Tests wird beispielsweise vom BSI in fünf Phasen eingeteilt, von denen für die Prävention von Konflikten vor allem die Vorbereitung und Abschlussanalyse wichtig sind<sup>70</sup>:

- ❖ Vorbereitung
- ❖ Informationsbeschaffung und –auswertung
- ❖ Bewertung der Informationen / Risikoanalyse
- ❖ Aktive Eindringversuche
- ❖ Abschlussanalyse;

*„Die Vorbereitungsphase beginnt mit der Definition des Ziels bzw. der Ziele des Penetrationstests“,* lautet die Empfehlung der BSI-Studie. Aber reicht das aus, um vermeidbaren Konflikten aus dem Weg zu gehen? Unter diesem Gesichtspunkt muss die Vorbereitungsphase früher ansetzen. Zunächst müssen wieder die Zwänge, Ziele, Prioritäten und Risiken der Betroffenen berücksichtigt werden, bevor man über die Ziele des Penetrations-Tests sprechen kann. Wenn man Konflikte vermeiden oder konstruktiv führen will, muss der Mensch im Zentrum des Interesses stehen und nicht die Technik. Wenn man sich die vier Problemfelder aller Beteiligten betrachtet, wird man schnell feststellen, dass diese – wie so oft – nicht deckungsgleich sind. Sie sind unter Umständen sogar gegensätzlich: Der IT-Sicherheitsbeauftragte will, dass alle Schwachstellen gefunden werden und der Administrator will, dass möglichst keine gefunden werden. Der Datenschutzbeauftragte macht sich Sorgen um die personenbezogenen Daten, die während des Tests anfallen und der Chef will einfach nur hören, dass der Laden läuft. Diese unterschiedlichen Problemfelder müssen synchronisiert werden und erst dann kann man über die Ziele des Pen-Tests nachdenken. Bei diesem Vorgehen erkennt man das Konfliktpotential rechtzeitig und kann rechtzeitig darauf eingehen.

Neben den unterschiedlichen Phasen eines Tests kann man nach Black-Box und White-Box Tests unterscheiden. Neben den technischen Aspekten, die zu dieser Unterscheidung führen, gibt es auch einen ganz menschlichen: Black-Box Tests sind fair, White-Box Tests sind unfair.

Einen Penetrationstest, bei dem der Tester im Voraus keine Information über das zu testende Netz erhält, nennt man Black-Box Test. Dies entspricht der Perspektive eines echten Angreifers, beinhaltet aber den Nachteil, dass der Tester viele Lücken nicht findet, weil er mit ihnen nicht gerechnet hat. Anders beim White-Box Test, wo alle Informationen zum System vorliegen, die auch dem Unternehmen oder der

---

<sup>70</sup> Bundesamt für Sicherheit in der Informationstechnik; "Durchführungskonzept für Penetrationstests"; 2003; Seite 45 

Behörde vorliegen. Das ist aus Sicht eines Administrators einigermaßen unfair, weil ein echter Angreifer diese Informationen nicht hätte. Aus einem rein technischen Blickwinkel sind White-Box Tests natürlich sinnvoller, weil sie mit einiger Wahrscheinlichkeit mehr Schwachstellen aufdecken. Betrachtet man die Sache jedoch durch die Brille der Administratoren, deren Systeme während des Tests „auf Links“ gedreht werden, erkennt man leicht das Konfliktpotential.

| Art des Tests | Black-Box                                                                                                                                                                                                                           | White-Box                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Philosophie   | <p>Überprüfen eines Systems gegen die Anforderungen aus den Sicherheitskonzepten.</p> <p>Nur das Außenverhalten des zu testenden Systems wird herangezogen und bewertet.</p> <p>Test aus der unwissenden Angreifer-Perspektive.</p> | <p>Überprüfen eines Systems auf Grundlage von Kenntnissen über die innere Funktion.</p> <p>Auch das „verborgene“ Innenverhalten wird herangezogen und bewertet.</p> <p>Test aus der Angreifer-Perspektive mit Insider-Wissen.</p> |
| Vorteile      | <p>Bessere Beurteilung des Gesamtsystems bei realen Angriff-Szenarien möglich.</p> <p>Beurteilung der zu Grunde gelegten Konzepte möglich.</p>                                                                                      | <p>Mit geringerem organisatorischen Aufwand verbunden.</p> <p>Schnellere, detailliertere Ergebnisse.</p>                                                                                                                          |
| Nachteile     | <p>Größerer organisatorischer Aufwand.</p> <p>Interne Fehler können leicht übersehen werden, wenn noch keine Angriffsvarianten dazu bekannt sind.</p>                                                                               | <p>Erfüllung der Anforderungen aus den Sicherheitskonzepten muss zusätzlich überprüft werden.</p> <p>Kann als „unfair“ empfunden werden.</p>                                                                                      |

**Tabelle 3-5:** Gegenüberstellung Black-Box und White-Box Test

In der Summe gibt es bei Pen-Tests also einiges, was man falsch machen kann. Daher sollen die bisher gemachten Überlegungen mit einem Fallbeispiel aus der ExAmple AG erläutert werden.

### 3.4.2.3 Fallbeispiel: Live-Vorführung und Pen-Test in der ExAmple AG

Die Sicherheitsexperten der ExAmple AG, Alice (Datenschutz), Bob (IT-Sicherheitsbeauftragter) und Dave (Werkssicherheit), hatte ein gemeinsames Ziel festgestellt. Sie sind sich einig:

*„Wir brauchen mehr Unterstützung vom Chef!“ Und Dave hatte gesagt: „Wir müssen ihm die Sache so schildern, dass er von selbst drauf kommt, dass wir seine Unterstützung brauchen!“*

Bob hatte nun den Vorschlag, dass ein Pen-Test weiterhelfen könnte. Dann wäre nicht immer er der Überbringer der schlechten Nachrichten und der Chef würde *„von neutraler Seite die Misere mal schwarz auf weiß geschildert bekommen“*. Auf der anderen Seite möchte er dabei den Erfolg seines Website-Projekts nicht gefährden, mit dem er beim Vorstand endlich mal Punkten kann. Dave sieht das Problem ähnlich: Da sich auch die Administratoren in der Vergangenheit mehr um die Neueinführung von Applikationen kümmern mussten, als um deren Absicherung, würden sie bestimmt auch schlecht aussehen.

*„Wenn wir es ordentlich einfädeln, und uns richtig vorbereiten, klappt es vielleicht“, meint Alice. Sie hat auch schon eine Idee: „Wie wäre es, wenn wir in einem ersten Schritt ein Live-Hacking für den Vorstand veranstalten? Eine Vorführung, wie schnell durch einen kleinen Konfigurationsfehler die Systeme offen stehen können, könnte vielleicht dabei helfen, das grundsätzliche Verständnis zu wecken.“*

*„Da kommt doch sowieso keiner von den hohen Herren“, wirft Bob ein.*

*„Nicht, wenn wir nur vorführen, was uns interessiert. Wir müssen vorführen, was die Vorstände interessiert. Was das ist müssen wir noch rausbekommen“, erwidert Alice.*

Das bringt Bob auf eine Idee: *„Die Frau vom Chef hatte mich mal gefragt, wie sie sich vor Phishing schützen kann und sie hat gesagt, dass sie sich Sorgen wegen der Kinder macht, dass die nicht irgendwas runterladen und dann der Staatsanwalt vor der Tür steht.“*

Und Dave wirft ein: *„Der Technik-Vorstand ist doch Elektro-Ingenieur. Da könnte man den Versuchsaufbau vorführen, mit dem man Tastatursignale über die Stromversorgung abhören kann. Da haben wir alles im Labor dafür da. Das kann einer der Auszubildenden vorbereiten.“*

Alice ist begeistert von den Ideen und auch in Dave und Bob keimt Hoffnung auf, die Vorstände für das Thema Sicherheit begeistern zu können. Die drei haben mit ihren Ideen die eigenen Zwänge, Ziele, Prioritäten und Risiken in die Problemfelder der Vorstände übersetzt. Damit ist der erste Schritt getan.

Wenige Wochen später findet die Vorführung statt und die Vorstände sind begeistert. Der Chef hat sogar seine Frau und die zwei Söhne mitgebracht, damit die sich anschauen können, wie schlimm es um die Sicherheit im Allgemeinen bestellt ist. Als der Chef Alice, Bob und Dave nach der Veranstaltung fragt, ob denn auch alle Abteilungen gut mit ihnen zusammenarbeiten, damit *„so etwas nicht bei uns passieren kann“*, ist die Katze im Sack. Der Chef möchte nächste Woche mal genauer zum Thema Sicherheit in der ExAmple AG unterrichtet werden. Als Bob sich einen Ruck gibt und vorschlägt, die Sicherheit seines Website-Projekts durch ein unabhängiges Prüf-Team testen zu lassen, stimmt der sofort zu: *„Na klar. So etwas wie eben vorgeführt wurde, möchte ich bei uns natürlich nicht sehen. Das ist ja richtig spannend, was Sie drei da machen.“* Alice, Bob und Dave sind ihrem Ziel ein ganzes Stück näher gekommen, mehr Unterstützung vom Vorstand zu bekommen.



Natürlich wird es im Gegensatz zu dem Fallbeispiel in der Realität ein wenig schwieriger werden und insbesondere mehr Zeit in Anspruch nehmen, bis sich Veränderungen einstellen. Vielleicht zeigt die Analyse von Zwängen, Zielen, Prioritäten und Risiken in Ihrer speziellen Situation eine ganz andere Richtung an, die Sie einschlagen müssen. Mit der richtigen Strategie werden Sie Ihre Ziele bei der Geschäfts- und Behördenleitung auf diese Art sehr viel leichter erreichen können.

Werfen wir zum Schluss des Fallbeispiels noch einmal einen Blick zurück auf die Motivatoren. Sind diese vorhanden, führen sie zu Zufriedenheit; im Gegensatz zu den Hygienefaktoren, die zu Unzufriedenheit führen, wenn sie fehlen. Haben Alice, Bob und Dave richtig motiviert? Betrachten Sie die folgende Liste und versuchen Sie, sich die Frage selbst zu beantworten:

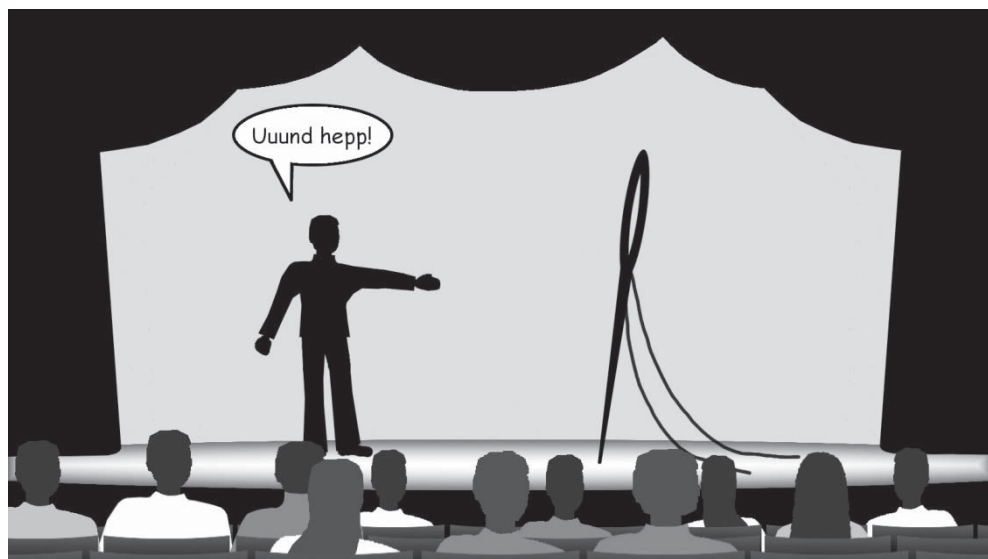
- ✓ Die Vorstände mit Motiven ausstatten, die diese vorher nicht hatten
- ✓ Deren vorhandenen Motiven zur Realisierung verhelfen
- ✓ Verhaltensweisen eine (subjektive) Bedeutung verleihen
- ✓ Anregen, begeistern, gewinnen

### 3.4.3 Motivation der Mitarbeiter

Wenn es darum geht, den einzelnen Mitarbeiter für Sicherheitsthemen zu motivieren, dann ist das sicher einfacher möglich, wie den einzelnen Chef. Das Problem entsteht hier eigentlich durch die Anzahl und den Umstand, dass es schon immer schwer war, es allen recht machen zu wollen. Für IT-Sicherheitsbeauftragte, Datenschützer und Co. ist es jedoch von besonderer

Bedeutung, alle Mitarbeiter zu erreichen. Eine Kette ist nur so stark, wie ihr schwächstes Glied: Das ist der Qualitätsmaßstab, der für Sicherheitsprofis gilt. Die Herausforderung besteht also darin, nicht weniger als 100% der Mitarbeiter zu motivieren. Da hilft der Schreck, den Live-Hackings oder Pen-Tests vermitteln nur wenig, wenn die nötige Handlungssicherheit nicht vermittelt wird. Während Geschäfts- und Behördenleitung vordringlich zu den richtigen Entscheidungen motiviert werden müssen, gilt es die Mitarbeiter ausgiebig zu schulen und die Arbeitsprozesse stets auf Praktikabilität hin zu untersuchen.

Auch, wenn man bei Mitarbeitern mit Live-Hackings und Pen-Tests die Ohren für das Thema Sicherheit öffnen kann, so ist es doch etwas anderes, sie dazu zu bringen, jeden Tag entsprechend der Sicherheitsrichtlinien zu arbeiten und im Zweifel bei den Sicherheitsexperten um Rat zu fragen. Mit einer Vorführung allein ist also nicht viel mehr erreicht, wie mit einem Strohfeuer, das schnell erlischt, wenn man nicht den einen oder anderen Scheid Holz auflegt. Das Live-Hacking ist also im besten Fall ein Teil eines großflächig angelegten „*Kommunikations-Konzepts*“ für die Sicherheitskultur. Drei Möglichkeiten, mit denen man für Handlungssicherheit bei den Mitarbeitern sorgen kann werden in diesem Abschnitt vorgestellt.



**Abbildung 3-16:** Für viele Mitarbeiter gleichen die Sicherheitsvorgaben dem biblischen Nadelöhr

Auch hier steht wieder im Vordergrund, möglichst viele Motivatoren zu aktivieren. Mitarbeiter sind sehr unterschiedlich und es gibt keinen Prototyp, auf den man seine motivierenden Anstrengungen zuschneiden könnte. Was den einen

Mitarbeiter motiviert, schreckt den anderen ab. Was beim einen Interesse weckt, lässt die anderen kalt. Das macht es nicht gerade einfach und lässt nur eine Herangehensweise zu: Mehrstufig, quasi mit Netz und doppeltem Boden und das Netz muss so engmaschig wie möglich gestaltet werden. Daher ist es bei Mitarbeitern zusätzlich nötig, sich den Hygienefaktoren zuzuwenden, die zu Unzufriedenheit führen.

Bei Mitarbeitern die Motivatoren *Erfolg, Anerkennung* und *Vorwärtkommen* über Sicherheitsmaßnahmen zu adressieren wird nicht funktionieren. Einzig für das Security-Team könnte darin ein Anreiz bestehen. Bessere Perspektiven bieten *Arbeitsinhalt, Verantwortung* und *Entwicklung*, obwohl sich die meisten Sicherheitsexperten scheuen, den Mitarbeiter mit einzubeziehen – gerade was die Verantwortung angeht. Gerade hier bieten sich jedoch Ansatzpunkte, Menschen für eine Sache zu begeistern. Auch im Verhaltenskreuz wird das Einräumen von Entscheidungsfreiheit bevorzugt. Beschneidet man Verantwortung und Entscheidungsfreiheit, hat das zusätzlich negative Auswirkungen auf die Hygienefaktoren *Dienstaufsicht, Verhältnis zu Vorgesetzten* und *Arbeitsbedingungen*.

Verantwortung und Entscheidungsfreiheit sollten also im Mittelpunkt der Mitarbeiter-Motivation stehen. Wenn man einem Kind die Gefährlichkeit von Schwimmbecken näherbringen will, wird es nicht ausreichen, ihm zu verbieten dort alleine hinzugehen. Und selbst, wenn man das Schwimmbecken einzäunt, wird das Kind sich irgendwann Gedanken darüber machen, wie es den Zaun überwinden kann – am besten ohne die nörgelige elterliche Obhut. IT-Sicherheitsbeauftragte, Datenschützer und Co. haben gegenüber den Eltern einen entscheidenden Vorteil: Sie haben es mit Erwachsenen zu tun. Keine Angst, auch meine Erfahrung hat manchmal die Frage aufgeworfen, ob es wirklich so ist. In solchen Einzelfällen kann man es dann ja immer noch mit einem Verbot probieren. Leider zeigt die Erfahrung auch, dass man damit in diesen Einzelfällen ebenso wenig erreicht, wie mit dem Zaun ums Schwimmbad. Die Phantasie von Mitarbeitern beim Umgehen von Sicherheitsmaßnahmen ist ebenso grenzenlos, wie die Phantasie von Gefängnisinsassen bezüglich ihres Ausbruchs. Dass sich viele Mitarbeiter im System der IT-Security tatsächlich wie in einem Zwangssystem fühlen und nach Ausbruchsmöglichkeiten suchen, hat die Studie *Entsicherung am Arbeitsplatz*<sup>71</sup> eindrucksvoll aufgezeigt: „Ein 100% dichtes Unternehmen ist seelisch nicht auszuhalten. Wie in einem modernen Neubau mit Mehrfachverglasung wuchert hier der Schimmel schon nach kurzer Zeit selbst auf glatten Oberflächen, sofern nicht ab und zu ordentlich durchgelüftet wird.“

---

<sup>71</sup> known\_sense (Herausgeber u.a.); *Entsicherung am Arbeitsplatz: Die geheime Logik der IT-Security in Unternehmen*; 2006; known\_sense; Seite 19 ff

In den folgenden drei Abschnitten soll ein Weg zu mehr Entscheidungsfreiheit und Mitarbeitermotivation aufgezeigt werden. Ausgehend von Awareness-Kampagnen, die die Mitarbeiter mit ins Boot holen sollen, werden im zweiten Abschnitt die Möglichkeiten kleiner Schupse besprochen, die die Entscheidungsfreiheit nicht einschränken, die Mitarbeiter aber in die richtige Richtung lenken sollen. Im dritten Abschnitt wird dargestellt, wie man Mitarbeiter für den Moment der Wahrheit wappnen kann, bei dem sie bei einer sicherheitsrelevanten Entscheidung auf sich alleine gestellt sind.

### 3.4.3.1 Awareness-Kampagnen

Mit Awareness-Kampagnen versucht man die Sicherheitskultur in Unternehmen positiv zu beeinflussen. Dabei wird ein möglichst breites Spektrum an Kommunikationskanälen genutzt, um – wie bereits gefordert – ein möglichst engmaschiges Netz zu spinnen, das alle Mitarbeiter erreicht und motiviert. Dazu muss der Kampagne vor allem ein funktionierendes Kommunikationskonzept zu Grunde liegen. Ein professionelles, aufeinander abgestimmtes und hochwertiges Erscheinungsbild ist ebenso wichtig, wie ein an das Unternehmen oder die Behörde angepasstes Vorgehen. Eine Awareness-Kampagne lässt sich nicht mit A4-Zetteln machen, die am Gebäudeeingang ausgelegt werden. Der Rückgriff auf Wissen aus Marketing und Kommunikationspsychologie ist daher unumgänglich.

Security-Awareness in einem Unternehmen der Pharma-Industrie funktioniert nicht nach denselben Gesetzmäßigkeiten wie in einer Behörde des Bundes. Das geht so weit, dass eine Kampagne, die in einem Unternehmen mit großem Erfolg durchgeführt wurde, in einem anderen auf taube Ohren stoßen kann. Bei der Gestaltung steht nicht die Technik im Mittelpunkt, sondern der Mensch. Auch wenn die Server und Risiken in der Pharma-Industrie und Bundesbehörden ähnlich sein mögen; auch wenn die Viren, die den Rechner eines Laboranten oder einer technischen Angestellten heimsuchen, gleich sind – die Menschen sind es sicher nicht. Und auch innerhalb eines Unternehmens sind nicht alle Mitarbeiter über einen Kamm zu scheren: Entwicklungsingenieure fühlen sich durch andere Dinge angesprochen wie Buchhalter. Diese Unterschiede müssen innerhalb der Kampagne berücksichtigt werden.

Da der Fokus einer Awareness-Kampagne auf den Menschen liegt, verwundert es nicht, dass Kommunikation der Erfolgsfaktor Nummer Eins ist. Das beginnt schon in der Vorbereitung, in der möglichst alle Protagonisten der Security-Bühne mit einbezogen werden müssen. Das ist schon allein deshalb notwendig, um eine Bestandsaufnahme der Sicherheitskultur zu machen und zu ermitteln, wie die Leute „ticken“. Fehlt die Unterstützung von einer Seite, oder sind sich alle einig, dass die Sicherheitskultur verbessert werden muss? Dass ist zwar nebensächlich, wenn man sich auf das zu vermittelnde Wissen konzentriert, nicht jedoch wenn

man sich ernsthaft mit den betroffenen Menschen auseinandersetzen will. Aus den bisherigen Überlegungen ergeben sich die folgenden Voraussetzungen für eine funktionierende Kampagne:

- ❖ Professionelles und hochwertiges Erscheinungsbild unter Rückgriff auf Wissen aus Marketing und Kommunikationspsychologie
- ❖ Einbindung aller Beteiligten der Security-Bühne, insbesondere der Geschäfts- oder Behördenleitung und der Interessenvertretungen
- ❖ Berücksichtigung der unterschiedlichen Personengruppen durch angepasste Kampagnen-Teile

Der Planungsaufwand für eine Awareness-Kampagne ist daher nicht zu unterschätzen und kann durchaus den größten Einzelposten ausmachen – durchaus vergleichbar mit einem Feuerwerk, dessen Vorbereitung Tage dauern kann, auch wenn es dann in nur wenigen Minuten abgefeuert wird. Wer motivieren will, der muss anregen, begeistern und gewinnen. Das funktioniert aber nicht, wenn man nach der ersten Leuchtrakete zwei Stunden auf die nächste warten muss. Auf diese Art verpufft die Begeisterung, ohne dass sie in den Folgeschritten für die Wissensvermittlung genutzt werden kann. Daher sollte die Kampagne gut vorbereitet und dann entlang eines Phasenverlaufs durchgeführt werden.

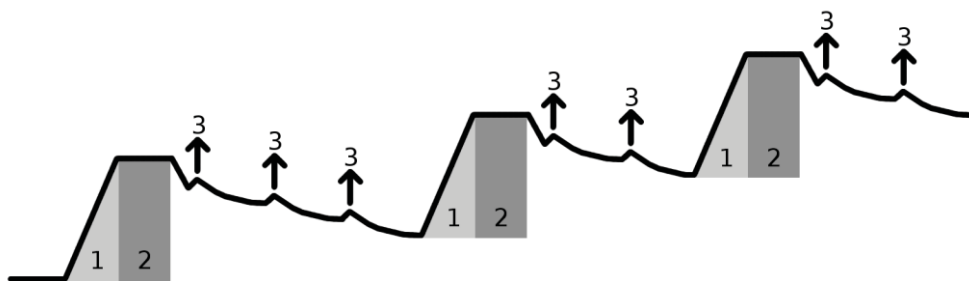
In der **1. Phase** geht es darum, möglichst viel Aufmerksamkeit zu generieren und dem Kind einen Namen zu geben. Die Unternehmensleitung sollte durch ein Anschreiben den Startschuss geben und die Zielsetzung erläutern, die mit der Kampagne verbunden ist. Vielleicht gab es einen Anlass, der die Kampagne erforderlich gemacht hat und ein Ziel, das erreicht werden soll. Wenn man die Mitarbeiter motivieren will, kann es nur gut sein, zu erläutern, was die Geschäfts- oder Behördenleitung motiviert. Es gibt überall Mitarbeiter die bei allen Dingen zunächst überprüfen, wie die Chefs dazu stehen, um dann die eigene Position festzulegen. Auf diese Art fahren Sie – ganz ohne Anstrengung – die ersten Erfolge ein. Alles was Sie tun müssen ist, dem Chef einen unterschiftsreifen Brief an die Mitarbeiter vorzulegen. Am besten einen, der die Unterstützung der Personal- und Interessenvertretungen genießt.

Der Startschuss wird von einer ganzen Reihe von Materialien begleitet, die nur einen Zweck haben: Die Kampagne muss ein wiedererkennbares Gesicht bekommen, so dass ihr alle weiteren Anstrengungen zweifelsfrei zugeordnet werden können. Flyer, Plakate und Give-Aways enthalten zunächst kaum Informationen und auch Artikel in Mitarbeiter-Zeitungen oder auf Intranet-Homepages stellen die Kampagne nur vor – die inhaltliche Arbeit erfolgt danach.

Die **2. Phase** dient der Wissensvermittlung und bildet den Schwerpunkt der Kampagne. Das zuvor aufgebaute Interesse am Thema Security muss jetzt bedient werden, bevor es wieder verfliegt. Die einzelnen Teile dieser Phase müssen auf die zuvor identifizierten, unterschiedlichen Personengruppen zugeschnitten sein. Vorträge und Live-Vorfürhungen müssen zielgruppenorientiert angeboten werden. Für Mitarbeiter im Außendienst empfehlen sich Web-basierte Trainings. Mit Workshops können kleinere Gruppen angesprochen werden und in Einzel-Coachings können besonders sicherheitsrelevante Positionen gezielt bedient werden. Eine weitere Möglichkeit bilden Wettbewerbe, an denen sich jeder beteiligen kann. Erwarten Sie dabei aber nicht zu viel Euphorie. Es sollte wirklich einfach sein teilzunehmen, damit man jeden erreicht.

Denkbar wäre zum Beispiel eine Postkarten-Aktion an jeden Mitarbeiter, die mit der Hauspost an das Security-Team zurückgeschickt werden kann. Alles was man tun muss, ist den Satz „*Security in der ExAmple AG heißt für mich ...*“ zu vervollständigen. Der Gewinner wird von einer Jury ermittelt und die besten Sprüche in einer Plakat-Aktion verwertet, die in der dritten Phase der Kampagne durchgeführt werden kann. Die Anzahl und Qualität der zurückgeschickten Karten wird sich übrigens erheblich steigern, wenn einer der Juroren der Geschäftsführer oder die Dienststellenleiterin ist.

Schwerpunkt der **3. Phase** ist die Verfestigung der erreichten Position. Nach dem erlebnisreichen Mittelteil der Kampagne wird das Interesse an Sicherheitsthemen meist früher als später nachlassen. Das ist erstens nicht verwunderlich – haben die meisten Mitarbeiter doch andere Dinge zu tun – und zweitens nicht so schlimm, wie auf den ersten Blick vermutet. Wenn man durch Awareness-Kampagnen erreichen kann, dass die Sicherheit in einer Wellenbewegung stetig steigt ist einiges gewonnen.



**Abbildung 3-17:** Anstieg der Sicherheit jeweils entlang der drei Phasen einer Awareness-Kampagne – Phase 3 stabilisiert bisherige Erfolg

Dazu muss jedoch verhindert werden, dass die Welle langsamer zurückgeht, als sie steigt. Die ganze Anstrengung war umsonst, wenn in der Folge nicht

regelmäßig aufgefrischt wird und man stattdessen auf den Status quo ante zurückfällt. Security-News-Letter, ein Security-Jour-fixe, eine Kolumne in der Mitarbeiterzeitung oder ein Kalenderblatt mit Sicherheitsvorfällen sind mögliche Ansätze. Mit Broschüren können einzelne Aspekte aufgefrischt oder vertieft werden. Wo das nötig ist, ergibt sich aus der Bewertung des Erfolgs in der zweiten Phase. Insbesondere für erfolgreiche Kampagnen bietet es sich an, im Rahmen der Öffentlichkeitsarbeit einen „sozialen Druck“ aufzubauen, der vor einem Rückfall bewahrt.

Die hier gemachten Vorschläge können nur ein erster Gedankenanstoß sein, wie umfangreich man in Kampagnen für Sicherheit werben kann. Sie erhebt daher keinen Anspruch auf Vollständigkeit. In der folgenden Tabelle sind die drei Phasen und ihre möglichen Bestandteile zusammengefasst:

| Phase 1<br>Aufmerksamkeit/<br>Branding | Phase 2<br>Wissensvermittlung/<br>Education | Phase 3<br>Festigung/<br>Consolidation |
|----------------------------------------|---------------------------------------------|----------------------------------------|
| Startschuss durch<br>das Management    | Vorträge                                    | News-Letter                            |
|                                        | Live-Vorführungen                           | Security Jour fixe                     |
| Flyer                                  | Web-Trainings                               | Mitarbeiter-Zeitung                    |
| Plakate                                | Workshops                                   | Kalenderblatt                          |
| Give-Aways                             | Einzel-Coachings                            | Broschüren                             |
| Mitarbeiter-Zeitung                    | Wettbewerbe                                 | Öffentlichkeitsarbeit/ PR              |

**Tabelle 3-6:** Phasen einer Awareness-Kampagne

### 3.4.3.2 Kleine Schupse

Viele Menschen gehen davon aus, dass jeder Mensch richtig denkt und entscheidet – eine Sichtweise, die sich in der Figur des *homo oeconomicus* aus den Wirtschaftswissenschaften manifestiert. Dieser trifft seine Entscheidungen auf Grundlage von

- ❖ Maximierung des eigenen Gewinns,
- ❖ vollkommener Voraussicht und
- ❖ unendlich schneller Reaktionsfähigkeit.

Weiterhin gilt, nach dieser Theorie, das es ein homo oeconomicus nur mit Partnern zu tun hat, die über die gleichen Fähigkeiten verfügen.<sup>72</sup> Gehen wir in einem ersten Schritt davon aus, dass Mitarbeiter auch bei sicherheitsrelevanten Entscheidungen nach diesem Muster funktionieren und betrachten als Beispiel folgende Situation: Jeff aus der Forschungsabteilung unseres Pharma-Unternehmens ExAmple AG bekommt per Mail eine PDF-Datei zugeschickt. *„Forschung in die Ecke gedrängt: Veröffentlichungspflichten für Medikamentenstudien weiter verschärft“*, heißt es im Betreff. Wenn es sich bei Jeff um einen homo oeconomicus handelt, würde das bedeuten, dass er...

1. ...seinen Gewinn maximieren will und daher am Inhalt der PDF-Datei interessiert sein wird.
2. Ausgestattet mit vollkommener Voraussicht weiß Jeff, dass in der PDF-Datei nur eine alte Pressemitteilung zum Thema wiedergegeben wird und die Datei so manipuliert wurde, dass sie eine jedem bekannte Schwachstelle des PDF-Readers ausnutzt und einem Angreifer so Administrator-Rechte verschafft.
3. Durch die unendlich schnelle Reaktionsfähigkeit aller Beteiligten ist es möglich, dass Jeff sofort die deutsche Polizei informiert, die in Zusammenarbeit mit der US- Polizei unmittelbar nach Empfang der Mail den Wohnort des Straftäters ermittelt hat und diesen in Cincinnati verhaftet.

Da der Straftäter aus der Welt des homo oeconomicus ebenfalls über die vollkommene Voraussicht verfügt, will er nicht ins Gefängnis, sondern seinen Gewinn maximieren. Daher hat er die Mail natürlich nie verschickt, weil er ja wusste, dass er sofort verhaftet werden würde. Nach dieser Theorie gibt es also gar keine interessanten Mails, keine böartigen PDF-Dateien, und keine Jeffs, die sie anklicken könnten: Alle Sicherheitsprobleme wären gelöst.

Wir wissen, dass die Anwendung dieses Modells einen vielleicht zum Wirtschaftswissenschaftler macht, nicht jedoch zum IT-Sicherheitsbeauftragten oder Datenschützer. Natürlich gibt es jede Menge manipulierte PDF-Dateien und jede Menge Jeffs, die sie öffnen. Wir müssen bei der Gestaltung von Sicherheitsrichtlinien von fehlerbehafteten, echten Menschen ausgehen, die nicht mit unendlicher Weisheit, in Sekundenbruchteilen ihren Gewinn maximieren. Im Gegenteil: Echte Menschen öffnen manchmal mit unendlicher Ignoranz, drei Tage nach der Sicherheitsschulung, gegen besseres Wissen, unter Vernichtung des Quartalsgewinns der gesamten Firma eine PDF-Datei, in der nur für Potenzpillen

---

<sup>72</sup> Günter Wöhe; Einführung in die Allgemeine Betriebswirtschaftslehre; 1996; Vahlen; ISBN: 3800620928; Seite 45

geworben wird. Dass die Reaktionsfähigkeit der Ermittlungsbehörden bei weltweiten Straftaten nicht die beste ist, ist auch kein Geheimnis. Die Menschen mit denen IT-Sicherheitsbeauftragte, Datenschützer und Co. zu tun haben, entsprechen eher einem *homo carens securitate*<sup>73</sup>. Dieser trifft seine Entscheidungen auf Grundlage von

- ❖ hoher Risikobereitschaft bis hin zur Gefährdung des eigenen Gewinns und des Gewinns anderer,
- ❖ mangelhafter oder fehlender Voraussicht und
- ❖ einer Reaktionsfähigkeit, die weit unter der Reaktionsfähigkeit von Hackern, Crackern und Bot-Nets liegt.

Stellen wir uns vor, Dave und Bob treffen sich auf eine Partie Schach. Dave ist nicht so gut und er wird mit einer ziemlichen Wahrscheinlichkeit gegen Bob verlieren. Mit ein paar Tipps könnte seine Situation deutlich verbessert werden. Angenommen, Dave bekommt immer einen kleinen Schups, wenn er eine Figur auf ein angegriffenes Feld stellt, oder eine seiner Figuren von Bob angegriffen wird – mehr nicht. Dave muss immer noch selbst spielen und selbst entscheiden, er macht jetzt nur weniger Fehler. „*Möchten Sie wirklich den gesamten Ordner mit allen 157 Dateien löschen?*“ Das wäre ein solcher Schups. Oder: „*Der Ordner ExAmple\_AG ist zu groß für den Papierkorb. Soll wirklich der gesamte Ordner unwiderruflich gelöscht werden?*“ Einen homo oeconomicus würden diese Fragen nur aufhalten, für den homo carens securitate sind sie die letzte Rettung.

Das Buch Nudge<sup>74</sup>, der beiden Professoren Thaler und Sunstein beschäftigt sich ausführlich mit solchen und anderen Schupsen, die Menschen vor offensichtlichen Fehlern bewahren sollen, ohne sie in ihrer Entscheidungsfreiheit einzuschränken. Ein Beispiel aus dem Buch, dass auch in der Presse<sup>75</sup> zitiert wurde, stammt vom Flughafen Schiphol: Dort wurde in den Urinalen der Herrentoilette das Bild einer schwarzen Stubenfliege angebracht, gleich neben dem Abfluss. Das Ergebnis: Die Trefferrate erhöhte sich um 80%. Das Beispiel macht deutlich, worum es beim richtigen „*Schupsen*“ geht: Die Fliege ist ein Anstoß, keine Anordnung. Überlegen Sie sich, wie hoch die Erfolgsquote einer flughafenweiten Anordnung zum

---

<sup>73</sup> Der Mensch, der am Mangel an Sicherheit leidet (Übersetzung: Johannes Lohscheidt)

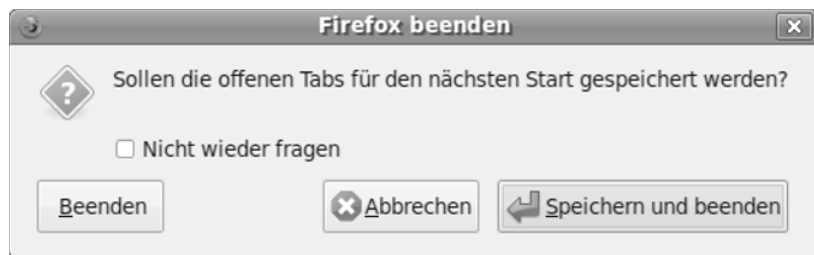
<sup>74</sup> Richard H. Thaler, Cass R. Sunstein; Nudge: Wie man kluge Entscheidungen anstößt; 2009; Econ; ISBN 978-3-430-20081-3

<sup>75</sup> Welt am Sonntag; 07.09.2008;  
[http://www.welt.de/wams\\_print/article2406700/Libertaerer-Paternalismus-Verfuehrung-zum-Guten.html](http://www.welt.de/wams_print/article2406700/Libertaerer-Paternalismus-Verfuehrung-zum-Guten.html)

besseren Zielen auf der Toilette gewesen wäre – bei Zuwiderhandlung mit Hausverbot belegt.

Im Abschnitt zum Verhaltenskreuz haben wir gesehen, dass das Einräumen von Entscheidungsfreiheit wichtig ist, um unnötige Konflikte zu vermeiden. Die Frage lautet nun, wie sich Menschen durch Sicherheitssysteme in eine Richtung schupsen lassen, ohne dabei ihre Entscheidungsfreiheit einzuschränken. Wie können Sicherheitsexperten das erreichen? Wie sieht eine „Sicherheitsfliege“ aus?

Wenn man viel mit dem Computer arbeitet zielt man tausende Mal am Tag auf Schaltflächen und Dialogfenster. Bei deren Gestaltung durch den Programmierer sollten nicht nur Gesichtspunkte der Anwendungsfreundlichkeit einfließen, sondern auch Sicherheitsaspekte eine Rolle spielen. Betrachten Sie das folgende Dialogfenster aus dem Firefox-Browser. Man bekommt es angezeigt, wenn man mehrere sogenannte Tabs mit Web-Seiten geöffnet hat und das Firefox-Fenster beenden will:



Auf die Frage „Sollen die offenen Tabs für den nächsten Start gespeichert werden?“ gibt es ja eigentlich nur zwei Antworten: „Ja“ und „Nein“. Wir sehen aber drei Schaltflächen, die auch noch ungleichmäßig angeordnet sind. Ist das Dialogfenster also schlecht gestaltet? Nein, es enthält einen kleinen Schups des Programmierers: Man liest den Fließtext von links nach rechts. Dort angekommen ist die „Ja“-Schaltfläche mit der Aufschrift „Speichern und beenden“ am nächsten, am größten und obendrein vorausgewählt. Entscheidet man sich vorschnell gegen das Speichern, klickt man vermutlich auf die vermeintliche „Nein“-Schaltfläche direkt daneben, der Dialog verschwindet und das Browser-Fenster bleibt weiter offen. Warum? Weil der Programmierer eine dritte Schaltfläche eingefügt hat, die das ganze Beenden abbricht und dem Anwender noch eine zweite Chance gibt. Die eigentliche „Nein“-Schaltfläche zum Beenden des Browsers steht am linken Rand des Dialogs. Auch das Kontrollfeld „Nicht wieder Fragen“ ist geschickt auf die linke Seite verbannt. Der Anwender wird quasi in eine Strafrunde zum Nachdenken geschickt. Wie müsste demnach ein Dialogfenster aussehen, das darauf hinweist, dass es gefährlich ist, extern zugesendete PDF-Dateien zu öffnen? Was halten Sie von diesem Vorschlag:



Dieses Dialogfenster würde viele zu einem Virenskan bewegen, ohne zu verhindern, die Datei auch ohne einen Scan zu öffnen – zum Beispiel wenn man sie schon einmal gescannt hat. Sicherheitsrelevante Anwendungen sollten systematisch nach diesem Prinzip gestaltet werden. Der Hinweis, dass 90% der Anwender vorher einen Virenskan durchführen, greift zu einem anderen psychologischen Trick: Thaler und Sunstein berichten in ihrem Buch von einem Fall aus Minnesota. Die Steuerbehörden wollten die Zahlungsmoral der Steuerzahler erhöhen und führten ein Experiment durch: Einigen Steuerzahlern sagte man, dass ihre Steuern für gute Zwecke verwendet werden würde, anderen sagte man, dass Steuersündern hohe Strafen drohen. Einer dritten Gruppe wurde mitgeteilt, dass bereits 90% der Bürger ihre Steuern ordnungsgemäß und vollständig bezahlt hätten. Die Zahlungsmoral verbesserte sich ausschließlich bei der dritten Vergleichsgruppe. Wenn Ihnen das zu manipulativ erscheint, können Sie statt „90% der Anwender...“ auch „*Schlaue Anwender...*“ verwenden. Die meisten Menschen wollen weder abseits stehen, noch zu den dummen Anwendern gehören. Das Fenster ohne einen Sicherheits-Schups könnte hingegen so aussehen:



Sie sollten in Ihrem Unternehmen oder Ihrer Behörde gezielt nach Möglichkeiten suchen, wie sie durch kleine Schups in die richtige Richtung eine Verbesserung der Sicherheitskultur erreichen können. Dabei ist allerdings Vorsicht geboten! Die Grenzen von einem kleinen Schups zur Manipulation sind fließend. Werfen wir also noch einmal einen Blick auf die Eigenschaften der Manipulation:

- ✗ Verschleierung von Tatsachen zum eigenen Vorteil
- ✗ Einseitige Begrenzung von Informationen oder Kontakten
- ✗ Unbewiesene oder unwahre Behauptungen

Sie sollten also nur schreiben, dass sich 90% der Anwender für einen Virensan entscheiden, wenn dem auch so ist. In jedem Fall ist es auch hier ratsam, die anderen Protagonisten der Security-Bühne so früh wie möglich mit ins Boot zu holen und das Vorgehen gemeinsam festzulegen.

### 3.4.3.3 „drive-by“-Risikoanalysen

Die Frage, wie wir Menschen Entscheidungen treffen ist wirklich spannend. Warum gibt es Menschen, die auf der einen Seite – z.B. der Bauingenieur Thomas – Brücken über hunderte Meter tiefe Schluchten bauen und sich auf der anderen Seite mit einer halb in Russisch geschriebenen Phishing-Mail die Zugangsdaten zu ihrer Bank stehlen lassen? Warum sind Menschen gleichzeitig so schlau und doch so dumm? Wir stützen uns bei unseren Entscheidungen auf zwei Systeme des Denkens: ein automatisches und ein reflektierendes.

| Automatisches System | Reflektierendes System |
|----------------------|------------------------|
| Unkontrolliert       | Kontrolliert           |
| Mühelos              | Angestrengt            |
| Assoziierend         | Deduzierend            |
| Schnell              | Langsam                |
| Unbewusst            | Bewusst                |
| Erlernt              | Regelgeleitet          |

**Tabelle 3-7:** Zwei kognitive Systeme<sup>76</sup>

Das reflektierende System tritt in Erscheinung, wenn sich ein Mensch schwierigen Entscheidungen stellt, wie z.B. Thomas, wenn er die Größe von Brückenpfeilern festlegt. Diese Entscheidung trifft er bewusst und kontrolliert. Auf Grundlage von genauen Bauvorschriften und statischen Berechnungen kommt er langsam und mit einiger Anstrengung zum Ziel. Wenn Thomas sich neben der Berechnung von Brückenpfeilern jeden Tag noch durch einen Berg von E-Mails klicken muss, kann leicht passieren, dass das automatische System die Oberhand gewinnt. Das Logo der Bank und das Corporate Design legen den Schalter um und schon werden die Zeilen mit dem russischen Akzent vom automatischen System ins Unterbewusste

<sup>76</sup> Richard H. Thaler, Cass R. Sunstein; Nudge: Wie man kluge Entscheidungen anstößt; 2009; Econ; ISBN 978-3-430-20081-3; Seite 34

verbannt. Mühelos kramt Thomas, wie schon hunderte Male zuvor, die Zettel mit den PINs und TANs heraus und gibt drei davon in das Eingabefeld der Web-Seite ein. Auf diese Weise klickt das automatische System für ihn alle Mails durch und er kann schnell wieder zurück zu seinen Berechnungen.

Würde Thomas die Gefahr erkennen, würde das reflektierende System ihn dazu veranlassen, die Mail genau zu prüfen und ihm würden die Rechtschreibfehler auffallen. Er würde merken, dass in der Adresszeile des Browserfensters nicht die Adresse seiner Bank steht, sondern eine ganz andere Domain und er würde merken, dass die Seite auch kein Sicherheitszertifikat zur Verfügung stellt. Er verlässt sich auf sein Bauchgefühl und sein automatisches System versendet die TANs.

Wie gut oder wie schlecht das automatische System entscheidet, liegt daran, wie gut es programmiert wurde. Fragen Sie einen beliebigen Mitarbeiter Ihres Unternehmens mit einer Skala von 1 bis 10, wie viel Angst er vor Phishing und Cross-Site-Scripting hat; und fragen Sie ihn, wie viel Angst er vor Terrorismus, Flugzeugabstürzen oder Spinnen hat. Der Bauingenieur Thomas würde vielleicht so antworten:

| Wie viel Angst haben Sie vor... | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---------------------------------|---|---|---|---|---|---|---|---|---|----|
| <b>Terrorismus</b>              |   |   |   |   |   |   |   |   | x |    |
| <b>Phishing</b>                 |   |   | x |   |   |   |   |   |   |    |
| <b>Flugzeugabstürzen</b>        |   |   |   |   |   |   |   |   |   | x  |
| <b>Cross-Site-Scripting</b>     |   | x |   |   |   |   |   |   |   |    |
| <b>Spinnen</b>                  |   |   |   |   |   |   |   | x |   |    |

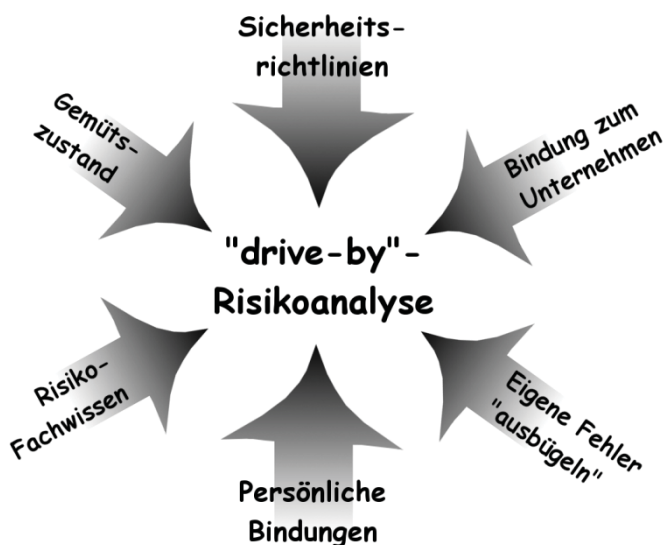
**Tabelle 3-8:** Mitarbeiterbefragung zur Angst

Wenn Thomas oft mit dem Flugzeug unterwegs ist, wird das automatische System die halbe Arbeit erledigen. Bei der Sicherheitskontrolle wird er automatisch den Gürtel ausziehen, die Uhr ablegen und den Schlüssel aus der Hosentasche nehmen. Am Gate zückt er geübt die Bordkarte, nimmt sich eine Zeitung, steigt ein, anschnallen, fertig. Dafür ist er bereits programmiert. Da er ein wenig Angst vorm Fliegen hat, hat er auch ein Programm, das fortwährend prüft, ob die Stewardessen nervös sind oder bereits ein Triebwerk raucht. Jemand, der keine Angst vor Flugzeugabstürzen hat, wird sein automatisches System eher auf den Tomatensaft oder das Essen ausgerichtet haben, um den Flug so angenehm wie möglich hinter sich zu bringen. Er würde keinen Grund sehen eine permanente

Risikoanalyse für einen Flugzeugabsturz durchzuführen, weil er das Risiko anders einschätzt.

Da Thomas nichts von Phishing weiß, hat er auch keine Angst davor und folglich auch kein Programm zur Verfügung, mit dem er bei jeder E-Mail, die etwas mit Zugangsdaten zu tun hat, eine Extrarunde für eine Risikoanalyse einlegt. Das ist bei vielen Sicherheits-Profis anders. Sie haben für praktisch jedes Risiko ein Programm parat, dass sie abspulen, weil sie so viele Risiken kennen. Bei manchem kann das in eine ziemliche Paranoia ausarten.

Diese Art von automatischen Risikoanalysen möchte ich „drive-by“-Risikoanalysen nennen. Sie werden nicht nach einem ausgeklügelten Vorgehensmodell durchgeführt, sie bestehen vielmehr aus mehreren Komponenten, mit denen Sie in der Vergangenheit programmiert worden sind. Nur eine davon entspricht den Sicherheitsrichtlinien des Unternehmens oder der Behörde (vgl. Abbildung 3-18). Hier muss sich zeigen, was aus den Flyern und den jährlichen Informationsveranstaltungen hängen geblieben ist. An der Komponente des aktuellen Gemütszustands und der Bindung ans Unternehmen lässt sich wenig ändern: Wer gut aufgelegt ist oder unter Stress steht, geht eben leichter mal ein Risiko ein und wem das Unternehmen egal ist sowieso. Bei den Komponenten Risiko-Fachwissen, persönliche Bindung und Umgang mit Fehlern können die Sicherheitsexperten jedoch noch einiges verbessern.



**Abbildung 3-18:** „drive-by“-Risikoanalyse: Sicherheitsrichtlinien und persönliche Bindung zum Sicherheits-Team müssen sich ergänzen

Am Einfluss der drei oberen Komponenten aus Abbildung 3-18 lässt sich wenig ändern. Was sich im Allgemeinen verbessern lässt, ist der Einfluss der unteren drei Komponenten: Risiko-Fachwissen, persönliche Bindung und das Verhalten bei eigenen Fehlern. Diese drei Komponenten lassen sich vor allem durch ein ausgeprägtes Vertrauensverhältnis zwischen Mitarbeitern und Sicherheitsexperten beeinflussen.

Wenn Thomas also mit Flugangst zu kämpfen hat, wird er damit besser zurechtkommen, wenn er die Besatzung der Maschine vertrauensvoll fragen kann, ob ein verdächtiges Klappern gefährlich ist, und ob es schlimm ist, dass er vergessen hat, sein Handy im Handgepäck aus zu machen. Ohne eine persönliche Bindung wird er sich den ganzen Flug über unnötige Gedanken über das Klappern machen und das Handy weiter eingeschaltet im Handgepäck in den oberen Staufächern liegen lassen – wird schon keiner merken. Seine „drive-by“-Risikoanalyse versagt systematisch, weil ihm der persönliche Draht zu jemandem fehlt, der sich mit Flugzeugen auskennt.

So geht es auch Mitarbeitern, die sich auf der einen Seite Gedanken darüber machen, Sicherheitsvorfälle verursacht zu haben, die es gar nicht gibt, diesen Sachverhalt aber für sich behalten, aus Angst den Arbeitsplatz zu verlieren oder gar ausgelacht zu werden.<sup>77</sup> Derartige Barrieren können nur durch ein gutes Vertrauensverhältnis zum Sicherheits-Team abgebaut werden. An dieser Stelle möchte ich erneut den IT-Grundschutz zitieren, der von IT-Sicherheitsbeauftragten fordert, dass *„Mitarbeiter davon überzeugt werden (müssen), dass ehrliche Antworten nicht zu Problemen für sie selbst führen.“*<sup>78</sup>

Das Security-Team muss für die Mitarbeiter des Unternehmens oder der Behörde immer ein vertrauenswürdiger Ansprechpartner sein, das nicht als das Problem, sondern als Teil der Lösung betrachtet wird. Die „Buhmann-Falle“, in der mancher Security-Profi feststeht, resultiert vielfach aus dem verklärten Bild, dass die Hacker die Freibeuter des Internets seien und IT-Sicherheitsbeauftragte, Datenschützer und Co. die Konquistadoren, mit denen man nur widerwillig zusammenarbeitet. Wer erreichen will, dass das automatische System der Mitarbeiter in wirklich brenzligen Situationen zuerst an das Sicherheits-Team denkt, der muss es in weniger brenzligen Situationen darauf trainieren.

---

<sup>77</sup> known\_sense (Herausgeber u.a.); Entsicherung am Arbeitsplatz: Die geheime Logik der IT-Security in Unternehmen; 2006; known\_sense; Seite 17

<sup>78</sup> Bundesamt für Sicherheit in der Informationstechnik; BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise; 2008; Seite 27 

### 3.4.4 Eigenmotivation und der Umgang mit Frustration

Die Karten stehen insgesamt nicht gut für Security-Profis. Eigentlich kann man nur verlieren und mancher hat sich nach einigen Jahren in der Branche schon gefragt: „Warum tue ich mir das eigentlich an.“ Viele geben irgendwann resigniert auf und nur die wenigsten halten über Jahrzehnte hinweg durch. Hat man das Personal und die Chefs endlich auf Kurs, ändern sich die Angriffsvektoren oder die Personalfluktuations frisst die erzielten Erfolge wieder auf. Wie motivieren sie sich immer wieder bei Null anzufangen?

Die Erfahrung zeigt, dass Sicherheitsexperten ihre Motivation kaum von außen beziehen. Was die klassischen Motivatoren angeht, sieht es nicht rosig aus: *Erfolg* hat man, wenn nichts passiert. Es ist wie im Fußball: Wenn ein Stürmer 90 Minuten tatenlos rumsteht und in der Nachspielzeit im Stolpern den Siegtreffer erzielt, ist er der Held des Tages. Der Torwart und die Abwehrspieler, die 90 Minuten lang glänzend gespielt haben und sich in der 91. Minute einen Fehler leisten, sind die Verlierer. Dementsprechend schlecht sieht es aus, was die *Anerkennung* angeht. Sie stellt sich erst mit der Dauer ein, wenn langsam klar wird, dass es nicht nur an den schlechten gegnerischen Stürmern liegen kann, dass die Mannschaft keine Gegentore kassiert.



Abbildung 3-19: Spaß am Job – nicht immer leicht

Die Motivatoren Erfolg und Anerkennung sind also einigermaßen ungeeignet, sich selbst zu motivieren: Der Erfolg ist schwer messbar und Anerkennung bekommt man nur für 100% Erfolg. Sinkt der Erfolg auf 99% und es kommt zum Sicherheitsvorfall, ist auch die Anerkennung dahin. Wenn man sich diesem

Erfolgsdruck aussetzt, kann schnell Frustration aufkommen, also Enttäuschung darüber, dass die erwartete Anerkennung durch den Chef oder die Mitarbeiter ausbleibt.

Gegentore im Fußball sind auch so eine Art Sicherheitsvorfall, und den Verteidigern geht es ähnlich wie den Security-Profis: Beide betreiben ein undankbares Geschäft, für das man sich entweder selbst, oder untereinander motivieren muss – sozusagen von Abwehrspieler zu Abwehrspieler. Welche Anerkennung wiegt wohl schwerer? Die vom Chef, der gar nicht richtig versteht, was er da anerkennt, oder die von Branchen-Kollegen, die genau wissen welche Anstrengungen hinter den Ergebnissen stecken?

Wenn Sie jetzt einwenden, dass die Anerkennung vom Chef ein gewichtiges Argument in Sachen Bezahlung und Verhältnis zu Vorgesetzten ist, dann haben Sie natürlich Recht. Die beiden Punkte *Bezahlung* und *Verhältnis zu Vorgesetzten* haben wir jedoch als sogenannte Hygienefaktoren kennengelernt: Diese motivieren nicht, wenn Sie vorhanden sind – einzig ihr Fehlen führt zu Unzufriedenheit. Es ist deutlich vielversprechender, sich Motivation unter gleichgesinnten Fachleuten zu holen. Sei es in der eigenen Firma oder Behörde oder auf Messen, bei Networking-Veranstaltungen oder in Internet-Communitys.



**Abbildung 3-20:** Anerkennung von den Kollegen ist wichtig

Der Kontakt zu Branchen-Kollegen ist aber nicht nur gut, um Anerkennung zu finden. Der Austausch mit Kollegen und die Teilnahme an Veranstaltungen bieten viele Möglichkeiten sich fachlich weiterzuentwickeln und von neuen Methoden und Ansätzen zu erfahren.

Vorausgesetzt, das eigene Unternehmen ist groß genug, bietet es sich an, regelmäßige Fachtagungen anzuberaumen, bei denen weniger die Wissensvermittlung oder ein bestimmtes Thema im Vordergrund stehen, sondern der Austausch mit den Kollegen. Eine Möglichkeit, mit der natürlich auch die Motivatoren Arbeitsinhalt, Verantwortung und Vorwärtsskommen angesprochen sind: Einen firmeninternen Fachkongress zu initiieren oder sich in der Unternehmenszentrale als Veranstalter anzubieten, macht neben Arbeit nicht nur Spaß, sondern empfiehlt für größere Aufgaben in der Zukunft. Eine derartige Veranstaltung lässt sich natürlich wunderbar mit einer Live-Vorführung verbinden, zu der man auch die Geschäfts- und Behördenleitung einladen kann. Auch wenn niemand kommt – wahrgenommen wird man in jedem Fall. Abschnitt 4.6 - *Tue Gutes und rede darüber* befasst sich eingehender mit diesem Ansatz.

Will man selbst herausfinden, was einen motiviert, muss man sich überlegen, welche Tätigkeiten in der Vergangenheit Freude bereitet haben und welche eher nicht. Welche Arbeit fiel einem leicht und was hat man eher auf die lange Bank geschoben? Wann war man guter Laune und wann hat man gereizt reagiert? Welche Aufgaben der Vergangenheit konnte man erfolgreich abschließen und wo ist man hinter den eigenen Erwartungen zurückgeblieben? Kurz: Welche Motivatoren und Hygienefaktoren kamen in der Vergangenheit zum Tragen? Diese Fragestellung lässt sich übersichtlich in einer persönlichen Lust-Frust-Bilanz<sup>79</sup> bearbeiten. Auf der einen Seite stehen Erlebnisse, die zur Zufriedenheit beigetragen haben und auf der anderen Seite die, die zu Unzufriedenheit geführt haben. Die Lust-Seite ist also die Seite Ihrer persönlichen Motivatoren, und die Frustseite die Ihrer Hygienefaktoren.

| <b>Lust-Seite</b><br><i>(Seite der Motivatoren)</i> | <b>Frust-Seite</b><br><i>(Seite der Hygienefaktoren)</i> |
|-----------------------------------------------------|----------------------------------------------------------|
| ...                                                 | ...                                                      |

**Tabelle 3-9:** Die persönliche Lust-Frust-Bilanz<sup>80</sup>

<sup>79</sup> Anita Bischof; Selbstmanagement: Effektiv und effizient; 2009; Rudolf Haufe Verlag, ISBN: 9783448093964; Seite 7

<sup>80</sup> Vordrucke zur Lust-Frust-Bilanz und zur Potential-Übersicht der Chancen und Risiken mit passenden Beispielen finden Sie im OnlinePLUS-Service zu diesem Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

An dieser Stelle geht es also nicht darum, die Untersuchungsergebnisse von Herzberg zu betätigen, die in Tabelle 3-3 dargestellt worden sind, sondern die Grundlage für Ihr ganz persönliches Motivationskonzept zu ermitteln. Mit einiger Wahrscheinlichkeit kann man davon ausgehen, dass Sie in Zukunft von denselben Dingen motiviert werden, wie in der Vergangenheit. Ausgehend von der persönlichen Lust-Frust-Bilanz, wie sie in Tabelle 3-9 dargestellt ist, werden nun für die Zukunft Tätigkeiten ermittelt, die das Potential haben, zu motivieren oder eher zum Gegenteil beizutragen. In einer Potential-Übersicht werden diese Chancen und Risiken dann gegenübergestellt:

| <b>Chancen-Potential</b><br>(Seite der Motivatoren) | <b>Risiko-Potential</b><br>(Seite der Hygienefaktoren) |
|-----------------------------------------------------|--------------------------------------------------------|
| ...                                                 | ...                                                    |

**Tabelle 3-10:** Die persönliche Potential-Übersicht der Chancen und Risiken

Die ermittelten Chancen entsprechen den Motivatoren, die in der eigenen Arbeit verborgen liegen, und die Risiken den Hygienefaktoren. Die zwei vorliegenden Gegenüberstellungen liefern Anhaltspunkte, wie man seinen Arbeitsbereich zukünftig gestalten sollte, auch wenn man sich leider nicht immer aussuchen kann, welche Aufgaben man in Zukunft angeht und noch weniger, welche man liegen lässt.

Frust entsteht vor allem dann, wenn man immer wieder in dieselben Messer läuft und von denselben Enttäuschungen getroffen wird. Als Sicherheitsexperte wird man Mitarbeiter und Chefs nur von einer Sache überzeugen können, wenn man selbst mit Begeisterung dabei ist. Daher ist die eigene Motivation durchaus als vordringliche Aufgabe zu betrachten, bei der man neben dem Beistand durch externe Fachkollegen insbesondere auch auf die Unterstützung im Security-Team zählen sollte. Wenn sich Datenschutzbeauftragte, Sicherheits- und IT-Sicherheitsbeauftragte gegenseitig im Weg stehen, ist nicht mehr viel Gegenwind aus der Chefetage nötig, um den Spaß an der Arbeit zu verlieren. Unter Umständen können Sie Ihre Kollegen im Security-Team dazu bewegen aus ihrer Sicht eine Lust-Frust-Bilanz und eine Potential-Übersicht zu erstellen, um nach Ähnlichkeiten zu suchen, für die sich eventuell auch ähnliche Lösungsansätze bieten. So wird Eigenmotivation nicht zu einem Problem fürs stille Kämmerlein, sondern zur Team-Aufgabe.

Auch, wenn Sicherheitsexperten eher im Hintergrund arbeiten und ihre Erfolge oft unsichtbar bleiben, so wissen wir doch, dass sie das Richtige tun, und für eine gute

Sache kämpfen. Als Held und Regisseur der Security-Bühne sind Sicherheitsexperten besonders dann erfolgreich, wenn sich Mitarbeiter und Chefs auf ihre Hauptrollen auf den anderen Bühnen des Geschäftslebens konzentrieren können. Das erfordert – neben allen anderen Anstrengungen – dass Sicherheitsexperten sich für ihre Erfolge selbst loben müssen, bevor sie sich in gewohnter Art mit der Suche nach Sicherheitsmängeln befassen und seitenlange Auflistungen erarbeiten, was sie alles noch nicht erreicht haben.

### 3.5 Zusammenfassung

Das Kapitel Konfliktprävention hat einen weiten Bogen gespannt. Im Mittelpunkt der Überlegungen stand die Frage, wie man das Thema Sicherheit an den Mann bzw. die Frau bringt. Grundvoraussetzung dafür ist es, eine gemeinsame Sprache zu sprechen, um sich nicht in einem babylonischen Sprach-Wirrwarr zu verlieren. Dass es für diese Forderung gerade für Sicherheitsexperten allerlei Grund gibt, haben wir gesehen und festgestellt, dass schon viel gewonnen ist, wenn man sich im eigenen Unternehmen oder der Behörde auf ein gemeinsames Vokabular einigen kann.

Mit der Konfliktpipeline wurde ein Modell vorgestellt, mit dem man sich gezielt auf Konflikte vorbereiten kann. Die unnötigen Teile sollen vermieden und die für die Lösungsfindung wichtigen Bestandteile sollen in geregelte Bahnen geleitet werden. So kann insbesondere vermieden werden, dass voreilig beigelegte Konflikte wieder aufkeimen, wenn einige Zeit vergangen ist: Der unterdrückte Wunsch von heute ist der Vorwurf von morgen. Nach dieser Formel ist es unter Umständen sogar nötig, die Argumente seines Gesprächspartners mit ins Feld zu führen, wenn dieser es nicht selbst tut. Konflikten wird so die emotional explosive Seite genommen und sie werden auf das reduziert, was sie im Kern sind: der Weg zur Lösung eines gemeinsamen Problems, in der sich alle Beteiligten wiedererkennen.

Wie schafft man es jedoch, Mitarbeiter und Chefs für Sicherheit zu begeistern, ohne den Umweg über konstruktive Konflikte gehen zu müssen? Wie stattet man jemanden gezielt mit Motiven aus, die dieser vorher nicht hatte? Ob Live-Vorführung, Penetration-Test, Awareness-Kampagnen oder kleine psychologische Schupse: Ziel ist es anzuregen und zu begeistern und den Mitarbeitern die Handlungssicherheit zu geben, die Lage auch dann richtig zu beurteilen, wenn sie in der einen oder anderen Situation die eingetretenen Pfade verlassen müssen, die Sicherheitskonzepte und Richtlinien vorgeben.

Wer all diese Herausforderungen erfolgreich meistern will, der muss nicht nur Chefs und Mitarbeiter motivieren, sondern auch für sich immer wieder die Kraft finden, sich dieser schwierigen Aufgabe zu stellen. Die meisten Sicherheitsvorfälle

wären einfach zu vermeiden und doch ist niemand davor gefeit, irgendwann zu den Opfern zu zählen. In solchen Frust-Situationen hilft oft nur der Beistand von vertrauten Kollegen aus der Branche, die dazu beitragen, die Rückschläge – die selbst den besten Sicherheitsexperten begegnen – im richtigen Licht zu betrachten.



## 4      Sicherheits-„Hebel“

*„Gebt mir einen festen Punkt im All,  
und ich werde die Welt aus den Angeln heben.“*

*Archimedes*

Wer eine stabile Tür aufstemmen will, muss einen langen Hebel ansetzen. Bei Aktienoptionen sind große Hebel gefragt und auch in vielen Kampfsportarten kommt man ohne gut platzierte Hebel nicht zum Erfolg. Hebel dienen dazu, der eingesetzten Kraft dadurch mehr Geltung zu verschaffen, dass man sie nicht direkt am Objekt ansetzt, das man zu bewegen sucht, sondern über einen Hebelpunkt, der die Kraft am Objekt verstärkt. Auch für Sicherheitsexperten gibt es eine Reihe von Hebeln, mit denen sie sich ihre Arbeit erleichtern können.

Einige dieser Sicherheits-Hebel haben wir bereits im Abschnitt über Motivation kennen gelernt: Live-Vorführungen, Penetration-Tests und Awareness-Kampagnen. Sie sind mächtige Werkzeuge, mit deren Hilfe die zu vermittelnde Botschaft der Sicherheitsprofis mehr Gewicht bekommt – die Botschaft an sich bleibt die gleiche. Sicherheits-Hebel eignen sich nicht nur zur Steigerung der Motivation. Sie dienen als Kommunikationsbeschleuniger und verbessern so das Verständnis für Sicherheitsthemen. Sie sind in gewisser Weise die Marketing-Instrumente der Sicherheitsprofis: Je mehr man davon zur Auswahl hat, umso besser kann man Sicherheit in der konkreten Situation präsentieren. Daher gibt es auch keine besonders guten oder weniger geeigneten Hebel. Die Auswahl muss situativ erfolgen und auf den Analyseergebnissen aufbauen, die unter Anwendung der Instrumente aus den vorherigen Kapiteln erzielt werden.

Effektive und effiziente Kommunikationsmittel sind der Schlüssel zu einem konfliktfreien Arbeitsalltag, in dem Sicherheitsprofis nicht in der „Buhmann-Falle“ landen, sondern als wichtiger Bestandteil des Unternehmens oder der Behörde wahrgenommen werden. Das Ziel ist erreicht, wenn Mitarbeiter, Chefs und Security-Team zusammenarbeiten und nicht – wie so oft – gegeneinander. Mitarbeiter die das Security-Team austricksen wollen, müssen begreifen, dass sie den Ast absägen, auf dem sie sitzen.

## 4.1 Security by ...

In der Betriebswirtschaftslehre wird eine ganze Reihe von Management-Konzepten unter der Überschrift *Management-by* zusammengefasst.<sup>81</sup> Wichtige Konzepte sind zum Beispiel *Management by objectives*, bei dem Mitarbeiter und Chefs gemeinsam Ziele vereinbaren, *Management by exception*, bei dem Mitarbeiter in Normalsituationen und Routinefällen selbstständig entscheiden und Vorgesetzte nur in Ausnahmefällen eingreifen oder *Management by delegation*, bei dem Aufgaben durch den Chef an die Mitarbeiter delegiert werden.<sup>82</sup>

Das Konzept, nach der ein Unternehmen oder eine Behörde in Sachen Sicherheit vorgeht, ist sehr individuell und kann sogar von Abteilung zu Abteilung unterschiedlich sein. In der einen Abteilung gibt es klare Prozesse und Konzepte, während in der anderen Sicherheit weitgehend dem Zufall überlassen bleibt. Diese beiden Extreme werden in den beiden nächsten Abschnitten beschrieben.

### 4.1.1 Security by tradition

Gerade kleinere und mittlere Unternehmen und Behörden sind weit entfernt von dem Idealbild eines Information Security Management Systems (ISMS) mit einem funktionierenden Risiko-Management-Prozess, wie man es beispielsweise gemäß ISO 27001 umsetzen kann. Wenn es überhaupt Konzepte zu Datensicherung, Informationssicherheit oder ähnlichem gibt, so hinken diese regelmäßig den tatsächlichen Gegebenheiten hinterher. Die Konzepte dienen nicht als Planungsinstrument für die Realität, sondern werden bestenfalls nachträglich an die Realität angepasst. In vielen Fällen muss das nicht einmal heißen, dass die IT-Systeme und die Prozesse nicht sicher wären. Das Zustandekommen der Sicherheitseinstellungen der Server, der Prozesse usw. ist aber weder systematisiert noch dokumentiert.

*Security by tradition* entsteht. Aber auch, wenn Sicherheitsmaßnahmen nicht strukturiert geplant werden, so bedeutet das nicht, dass es keine gibt. Auch ohne Konzept und formalisierten Prozess kommt für jeden Windows-Administrator irgendwann die Frage, wie er die Passwortrichtlinien festlegen will oder welche Protokolldaten gespeichert werden sollen. Selbst, wenn er für die Passwörter keine Mindeststandards festlegt und keinerlei Systemereignisse mitprotokolliert, so ist das eine Sicherheitsentscheidung, die getroffen wird: Toleriert er die damit

---

<sup>81</sup> Übersicht in: Management-by-Konzepte: Akademische Schriftenreihe; Isabell Preisler, 2008; GRIN Verlag; ISBN: 9783640142149; Seite 5 ➤

<sup>82</sup> Henner Schierenbeck; Grundzüge der Betriebswirtschaftslehre; 2003; Oldenbourg Wissenschaftsverlag, ISBN: 9783486273229; Seite 156 ➤

verbundenen Risiken, oder toleriert er sie nicht? Ob der Server-Raum hinter einer nicht abschließbaren Glastür oder einer Brandschutztür mit Sicherheitsschloss liegt, irgendwann wurde diese Entscheidung getroffen und sie hatte Einfluss auf den Ist-Zustand der Sicherheit des Server-Raums.

Sicherheitsentscheidungen kann man nicht aus dem Weg gehen, selbst dann nicht, wenn man sich dagegen wehrt. Selbst das Aufschieben einer Sicherheitsmaßnahme ist eine Entscheidung gegen deren sofortige Umsetzung. In diesem Sinn gibt es auch in jedem Unternehmen und jeder Behörde eine Form von Sicherheitskultur, auch wenn damit weder ein Ziel verfolgt wird, noch nachvollziehbar oder gar messbar wäre, was bisher erreicht wurde und was nicht. Wenn es Sicherheitsmaßnahmen gibt, dann entweder aus Zufall oder aufgrund schlechter Erfahrungen, zum Beispiel mit Datenverlust oder Virenbefall. Irgendwann fängt jeder damit an, seine Daten zu sichern oder einen Virenschanner zu installieren. Spätestens dann, wenn die ganzen Viren, Würmer und Trojaner auf dem eigenen Rechner die Leitung ins Internet unbenutzbar gemacht haben. Diese Art der Sicherheitskultur ist historisch gewachsen: Security by tradition eben.

Im Einzelfall kann die Rechnung sogar aufgehen: Mit ein wenig Glück spart sich ein Unternehmen viel Geld für Sicherheitsmaßnahmen und Verwaltungsaufwand, ohne dass es je Opfer eines Angriffs wird, während andere Unternehmen, die viel Geld in Sicherheit investieren, ständig angegriffen und geschädigt werden. Das ist im Einzelfall nicht auszuschließen.

| Vorteile                      | Nachteile                           |
|-------------------------------|-------------------------------------|
| Schnelle Entscheidungsfindung | Sicherheit ist Glückssache          |
| Geringe bis gar keine Kosten  | Schadenspotential/ Risiko unbekannt |
| Kein Verwaltungsaufwand       | Keinerlei Dokumentation             |

**Tabelle 4-1:** Vor- und Nachteile von Security by tradition

Wenn Sie in so einem Umfeld arbeiten, benötigen Sie sehr große Hebel um Sicherheitsmaßnahmen durchzusetzen. Sicherheit bleibt dem Zufall überlassen und nicht zuletzt wegen der fehlenden Dokumentation ist es unmöglich Aussagen zu Schadenspotential oder Risiko zu treffen. Für Sicherheitsprofis mag die Vorstellung eines solchen Unternehmens grausig klingen – es gibt sie aber leider und das nicht zu knapp. Das liegt vor allem an den Kostenvorteilen, die unbestreitbar vorhanden sind, solange es keine Sicherheitsvorfälle gibt. Denken Sie an die Webseite der kleinen Schreinerei, die Kundendatenbank eines Kleinunternehmers oder das W-LAN der Arztpraxis. Solange nichts passiert, wird man die Firmeninhaber nicht von Updates für Webserver, einem Backup der

Kundendatenbanken oder besseren Passphrasen für die W-LAN-Verschlüsselung überzeugen können. Security by tradition ist daher die Art von Sicherheitskultur, von der man lieber sagen möchte, dass das etablierte System eine Un-Sicherheitskultur ist. Demgegenüber stehen Unternehmen und Behörden, in denen Sicherheit ein strukturierter und dokumentierter Prozess ist.

#### 4.1.2 Security by concept

*Security by concept* basiert auf Sicherheitskonzepten. Ausgehend vom einen Extrem, Security by tradition, handelt es sich hierbei um den Zielzustand. Zwischen diesen beiden Polen rangiert die Sicherheitskultur in jeder Organisation oder zumindest in Teilen davon. Macht man die Unterteilung klein genug, kann man für jede Sicherheitsmaßnahme feststellen, ob man sich by tradition oder by concept für oder gegen sie entschieden hat. Hängen mehrere Maßnahmen zusammen, so lässt sich dieser Zusammenhang auch wieder in eine der beiden Kategorien einordnen.

Man kann zum Beispiel auf dem Mail-Server einen Virens Scanner by tradition haben, weil er beim Provider mit im Lieferumfang enthalten war, oder man hat sich bewusst – also by concept – dafür entschieden. Gleiches gilt für die Virens Scanner auf den PCs, die den Mail-Verkehr ein zweites Mal überprüfen. Der Zusammenhang, dass nun jede Mail zwei Mal überprüft wird, kann ebenfalls by tradition entstanden sein oder eine bewusste Entscheidung by concept. Das kann durchaus sinnvoll sein, wenn beide Virens Scanner unterschiedliche Virensignaturen verwenden.

Security by concept beantwortet also nicht die Frage, ob eine Sicherheitsmaßnahme getroffen wurde oder nicht. Man kann durchaus by concept auf eine Sicherheitsmaßnahme verzichten und damit sogar ein hohes Risiko eingehen. Entscheidend ist, dass man zu dieser Entscheidung auf Grundlage eines analytischen Vorgehens gekommen ist. So kann ein Unternehmen, das einen nach ISO 27001 zertifizierten Risikomanagement-Prozess etabliert hat, durchaus schlechter abgesichert sein, wie ein Unternehmen in dem die Sicherheit traditionell gewachsen ist. Glauben Sie nicht? Nehmen Sie als Beispiel auf der einen Seite eine Spedition mit externem IT-Sicherheitsbeauftragten und sechs Monate altem ISO-Zertifikat fürs Rechenzentrum und auf der anderen Seite die nicht zertifizierten Server einer Unternehmensberatung die Live-Hackings und Penetration-Tests anbietet. Was denken Sie, welche Server sicherer sind?

Security by concept erhöht also nicht per se die Sicherheit. Durch analytisches Vorgehen schafft es aber auf jeden Fall Klarheit über Gefahren und Risiken und eine dementsprechend aussagekräftige Dokumentation. Diesen Vorteilen stehen höhere Kosten und ein größerer Verwaltungsaufwand gegenüber, durch den sich die Entscheidungsfindung verlangsamen kann. Die Vor- und Nachteile der beiden

Konzepte sind in Tabelle 4-1 und Tabelle 4-2 gegenübergestellt. Die Vorteile der einen Tabelle sind im weitesten Sinne die Nachteile der anderen und während die Vorteile von Security by tradition sich für Chefs sicher verlockend anhören, schrecken die Nachteile von Security by concept ab. Umgekehrtes gilt für Sicherheitsprofis.

| Vorteile                           | Nachteile                     |
|------------------------------------|-------------------------------|
| Analytisches Vorgehen              | Langsame Entscheidungsfindung |
| Gefahren und Risiken genau bekannt | Hohe Kosten                   |
| Aussagekräftige Dokumentation      | Hoher Verwaltungsaufwand      |

**Tabelle 4-2:** Vor- und Nachteile von Security by policy

Sie fragen sich sicher schon, was die beiden Security-by-Extreme zu einem Hebel macht. Durch die Augen eines Sicherheitsexperten kann man diese Frage nicht beantworten. Sie müssen dazu versuchen, die Brille eines Geschäftsführers oder eines Dienststellenleiters aufzusetzen und die folgende Gegenüberstellung betrachten, in der die Vor- und Nachteile von Security by tradition und by concept noch einmal gegenübergestellt sind. Sie sehen dort die Antwort eines Chefs auf die folgende Frage:

*„Wie um alles in der Welt konnten Sie die Umsetzung einer Sicherheitsmaßnahme ablehnen, wegen der es nun – unter Ihrer Führung – zu einem schwerwiegenden Sicherheitsvorfall gekommen ist?“*

| Security by tradition                                                                                                                                                                                                                                                                                                                                            | Security by concept                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><i>„Für mich standen schnelle Entscheidungsfindung, geringe Kosten und ein geringer Verwaltungsaufwand immer im Vordergrund. Das hohe Risiko kannte ich nicht und auch das Schadensausmaß hat mich überrascht. Leider wurden diese Dinge vom Sicherheits-Team nicht ordentlich dokumentiert. Zum Schluss hat uns dann auch noch das Glück verlassen.“</i></p> | <p><i>„Wir haben einiges für Sicherheit investiert, einen hohen Verwaltungsaufwand und lange Entscheidungswege auf uns genommen. Nach fundierten Analysen waren mir das Risiko und das mögliche Schadensausmaß genau bekannt. Mein Sicherheits-Team hat mir dazu regelmäßig Berichte vorgelegt und meine Entscheidung gegen die Maßnahme dokumentiert“</i></p> |

**Tabelle 4-3:** Security by concept beraubt Chefs ihrer mentalen Komfortzone, wenn sie Sicherheitsmaßnahmen ablehnen

Sicherheitsexperten müssen Security by tradition also nicht deshalb aus allen Ecken der Firma vertreiben, weil dadurch mehr Sicherheit entstünde, sondern weil Chefs auf diese Art ihrer mentalen Komfortzone beraubt werden, wenn sie sich das nächste Mal gegen eine Sicherheitsmaßnahme aussprechen, oder das Geld für eine Maßnahme zu knapp ist. Das ist ein sehr mächtiger Hebel, auch wenn man das nicht gleich auf den ersten Blick erkennt.

Nichts ist schlimmer als für die eigenen Entscheidungen die Verantwortung tragen zu müssen und nichts ist auf Dauer wirksamer, wie die Wahrscheinlichkeit zu erhöhen, dass es irgendwann mal soweit kommen könnte. Sicherheitsprofis erreichen das durch die Etablierung eines Sicherheits-Management-Prozesses, der Entscheidungen analytisch vorbereitet und sie dokumentiert. Ziel ist es, jedes tolerierte Risiko by tradition in eines by concept zu überführen.



Abbildung 4-1: Security by concept aus Sicht des Chefs

## 4.2 Good Cop – Bad Cop

Die Kommunikationssituation, in der sich die Sicherheitsexperten befinden, ist nicht die beste. Nicht immer kann man sich aussuchen, mit wem man zu welchem Thema kommunizieren möchte. Wer Sicherheit als Hauptaufgabe hat, verbringt naturgemäß einen großen Teil der Zeit mit Unsicherheit: Allzu oft sind es schlechte Nachrichten, die man zu überbringen hat und mancher leidet das Schicksal der Cassandra aus dem antiken Griechenland, die zwar gegen Ende des Trojanischen

Krieges den Angriff mit dem Trojanischen Pferd vorhergesehen hatte, deren Warnungen jedoch ungehört blieben.<sup>83</sup>

Gespräche über Unsicherheit, Gefahr und Risiken kann man als Sicherheitsprofi nicht umgehen, sind sie doch der eigentliche Grund, warum man seinen Job bekommen hat. Kein Sicherheitsbeauftragter wird eingestellt, um alles schön zu reden. Chefs und Mitarbeiter möchten schon wissen, wo der Schuh drückt, und aus welcher Richtung Gefahr droht. Sie wollen es nur nicht so oft gesagt bekommen, dass sie es irgendwann nicht mehr hören können. Nichts ist schlimmer, als nur noch von Gefahren, Richtlinien und Verboten zu sprechen.

Woher also gute Nachrichten nehmen und wie über die schlechten sprechen, ohne dem Cassandra-Syndrom anheim zu fallen? Wie verschafft man sich Gehör innerhalb der Unternehmen oder der Behörden, für die man tätig ist? Wie findet man die richtige Mischung aus guten und schlechten Nachrichten? Gute und schlechte Nachrichten stehen sich als gegensätzliche Pole gegenüber und ergänzen sich in ihrer Wirkung. Wer in eine thematische Monotonie verfällt, verliert mit der Zeit die Aufmerksamkeit der Zuhörer.

#### **4.2.1 Positive Nachrichten generieren**

Zuerst stellt sich die Frage, wie man in die Rolle des Good Cop kommt, der versucht, mit guten Nachrichten Einfluss zu nehmen. Eigentlich gar nicht so schwer, wenn man es schafft, den Fokus von den Sicherheitskonzepten, Betriebsvereinbarungen und Service Level Agreements zu nehmen und sich mehr mit der sozialen Seite der Security zu befassen. Wer positive Nachrichten unter die Leute bringen will, der muss Spaß daran finden, sie zu erzählen.

Es gibt viele positive Nachrichten im Bereich Sicherheit – sie stehen nur nicht im Fokus vieler Sicherheitsprofis, weil sie darauf zu wenig achten. Man soll ja die Gefahr im Auge behalten und die eigenen Leute vor schlimmen Vorfällen bewahren und nicht davon erzählen, welche Gefahren bereits gebannt sind. Dabei ist es wichtig, auch davon zu berichten, welche Erfolge man bereits erzielt hat.

Jeden Tag kann man in der Zeitung oder den einschlägigen Online-Portalen von neuen Angriffsvarianten und Sicherheitsvorfällen lesen.<sup>84</sup> Die Nachrichten, die man dort findet, sind nicht nur interessant, wenn sie eine neue Bedrohung

---

<sup>83</sup> Der griechische Gott Apollon hatte Cassandra aus Liebe die Gabe der Vorhersehung geschenkt. Da sie seine Liebe nicht erwiderte, belegte er ihre Vorhersehung mit dem Fluch, auf immer ungehört zu bleiben.

<sup>84</sup> Eine Link-Liste mit hervorragenden Security-Blogs und News-Portalen in englischer und deutscher Sprache finden Sie im OnlinePLUS-Service zu diesem Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

aufzeigen, sondern auch dann, wenn man bereits vor einer der genannten Bedrohungen geschützt ist:

Wenn man beispielsweise bei der Entscheidung für oder gegen eine bestimmte Software auch sicherheitstechnisch richtig lag, weil die abgelehnte Software durch eine Reihe von Sicherheitsmängeln in Erscheinung tritt, dann ist das durchaus erwähnenswert. Zum Beispiel so:

*„Entscheidung für X-Tool goldrichtig:  
Y-Tool mit mehreren Sicherheitslücken in den Schlagzeilen!“*

Ähnliche Nachrichten lassen sich aus anderen Sicherheitsvorfällen generieren. Zum Beispiel zu einem Vorfall mit einem gestohlenen Laptop:

*„Datenskandal nach Laptop-Diebstahl in XY GmbH:  
Unsere Laptops durch Festplattenverschlüsselung geschützt!“*

Auch ist es eine gute Nachricht, wenn man die Gefahr schnell abwenden konnte, die von einer neuen Sicherheitslücke ausging:

*„Nur 2 Stunden nach Bekanntwerden der neuen Sicherheitslücken im Betriebssystem:  
Unsere Server bis auf weiteres durch Work-Around vor Angreifern geschützt!“*

Viele Sicherheitsprofis haben mit der Zeit ein Gespür dafür entwickelt, wo sie suchen müssen, um Schwachstellen und menschliches Fehlverhalten zu finden. Es liegt auf der Hand, dass bei dieser Methode meist schlechte Nachrichten entstehen und Mitarbeiter irgendwann denken, dass sie ohnehin immer wieder verlieren. Eine Möglichkeit das zu verhindern ist es, Kontrollen durchzuführen, bei denen Sie vorher wissen, dass alles in Ordnung ist. Gönnen Sie den Mitarbeitern auch Mal das schöne Gefühl, bei nichts erwischt worden zu sein, auch wenn die Versuchung noch so groß für Sie ist. Insbesondere sollten Sie das Lob für die Einhaltung von Sicherheitsvorschriften ohne Einschränkungen gelten lassen und es nicht durch einen nachgeschobenen Tadel relativieren. Auf diese Weise können Sie die Mitarbeiter in dem bestärken, was schon gut läuft und sie ermuntern, nicht nachzulassen: So übernehmen Sie die Rolle des Good Cop.

In vielen Fällen wird das eine Suche nach dem Trivialen sein. Nicht alles was einem Sicherheitsprofi trivial erscheint, ist für Mitarbeiter und Chefs auch trivial. Genauso wenig, wie die Meisten mit Absicht gegen Sicherheitsrichtlinien verstoßen, halten sie sich bewusst daran. Gewisse Abläufe werden einfach so erledigt, wie sie schon immer erledigt wurden. Nicht, weil sie so im Sicherheitskonzept stehen. Daher lohnt es sich durchaus, die Betroffenen dafür zu

loben, wenn sie sich an die Standards halten, weil das vielen in der konkreten Situation gar nicht bewusst ist – und wenn doch: Umso besser.

Berichten Sie über umgesetzte Sicherheitsmaßnahmen – auch dann, wenn sie Ihnen nicht nennenswert erscheinen. Der Microsoft Patch-Day zum Beispiel kann gleichzeitig als gute Nachricht dienen, ohne dass dabei vergessen wird, dass damit nicht alle Sicherheitsprobleme gelöst sind:

*„Microsoft Patch-Day: X Sicherheitslücken geschlossen.  
Ein Hersteller-Patch für die Y-Schwachstelle lässt trotzdem weiter auf sich warten.“*

Wenn man sich seiner Sache einigermaßen sicher ist, kann man versuchen einen weitreichenden Schritt zu gehen und eine Zertifizierung anstreben. Damit schafft man eine Möglichkeit, sich die guten Nachrichten von externer Seite Schwarz auf Weiß bestätigen zu lassen. Man muss hierbei zwei Arten von Zertifikaten unterscheiden: Solche für Personen und solche für Organisationen.

Die Zertifizierung von Organisationen bietet sich vor allem für kleinere Teilbereiche im Unternehmen oder der Behörde an, zum Beispiel das Rechenzentrum. Man sollte jedoch nicht dem Irrtum unterliegen, auf diese Weise einfach zu positiven Nachrichten zu kommen. Im Gegenteil: Zertifizierungen sind mit großen Anstrengungen verbunden – selbst dann, wenn sie nur einen abgegrenzten Teilbereich betreffen. Der Weg von der Idee bis zum Zertifikat ist steinig und kann sich schnell bis zu einem Jahr oder darüber hinaus hinziehen. Als Person kann man ebenfalls Zertifizierungen anstreben, die ein gewisses Maß an fachlicher Expertise bescheinigen und ebenfalls geeignet sind, mit guten Nachrichten aufzufallen.

Das folgende Fallbeispiel soll einen Ansatz liefern, wie man sich im Sicherheitsteam gezielt darauf konzentrieren kann mehr positive Nachrichten zu generieren und diesen auch Gehör zu verschaffen. Die Sicherheitsexperten der ExAmple AG, Alice, Bob und Dave führen dazu ein Brainstorming der guten Nachrichten durch.

#### 4.2.1.1 Fallbeispiel: Alles bestens in der ExAmple AG

In der ExAmple AG hat sich eine schlechte Stimmung gegen das Sicherheitsteam zusammengebraut. Mitarbeiter und Management können nichts mehr von Virenwarnungen, Sicherheitsvorfällen und sonstigen schlechten Nachrichten hören. Bei manch einem haben sich wegen der vielen schlechten Nachrichten der letzten Zeit die Ohren schon auf Durchzug gestellt: Datenskandal hier, schwache Passwörter da.

Der IT-Sicherheitsbeauftragte Bob, die Datenschutzbeauftragte Alice und der Sicherheitsbeauftragte Dave haben sich entschlossen, der schlechten Stimmung entgegenzuwirken, indem sie bewusst für positive Nachrichten sorgen. Sie setzen sich zusammen, um über ihre Lage zu sprechen. Alice beginnt:

*„OK Jungs, vielleicht haben wir in letzter Zeit den Bogen ein wenig überspannt. Ich bin auch nach jedem Datenskandal, der durch die Presse ging, zum Vorstand gerannt und hab' ihm erzählt, dass das bei uns auch jederzeit passieren kann. Klar, dass der mich jetzt immer schon mit den Worten >Was is' es denn diesmal?< begrüßt. Rauskommen tut bei den Gesprächen fast gar nichts mehr.“*

*„So kommt es mir auch vor“, hakt Bob ein. „Ich glaube, wir haben ihn ein wenig abgestumpft. Ich bin ja auch nur noch mit schlechten Nachrichten auf der Bildfläche erschienen. Den Titel größter Arbeitsverhinderer hatte ich ja schon – jetzt bin ich der größte Arbeitsverhinderer mit Cassandra-Syndrom.“*

*„Ihr habt schon recht“, sagt Dave. „Aber ist es nicht unsere Pflicht, den Chef über die Risiken aufzuklären? Wir sind ja nicht die Marketing-Abteilung: Die sind doch fürs Schönreden zuständig, nicht wir.“*

Alice lässt nicht locker: *„Es hilft nichts. Wenn wir immer nur schlechte Nachrichten verbreiten, hört man uns nicht mehr zu. Wir müssen auch mal was Positives berichten. Nur so erreichen wir, dass der Chef den Unterschied merkt, wenn wir auch Mal ne schlechte Nachricht haben.“*

Alice, Bob und Dave machen eine Liste mit Möglichkeiten, wie sie in den nächsten Wochen gezielt gute Nachrichten generieren können, und eine, über welche Medien sie verbreitet werden sollen (Abbildung 4-2). Die Idee einer Kunden-Info findet Alice recht reizvoll. Vielleicht können sie den Chef davon überzeugen, sich mit den Sicherheitsbemühungen der ExAmple AG bei den Kunden zu empfehlen.

Alice schlägt vor: *„>Sicherheitsteam der ExAmple AG ist Angreifern immer einen Schritt voraus!<, das wäre doch eine nette Überschrift.“*

*„Mir wird schlecht“, stöhnt Bob skeptisch. „Und was wenn nicht?“*

*„Nichts da“, unterbricht Alice. „Du hast es mit Deinem Zertifikat doch international anerkannt und Schwarz auf Weiß: Du bist ein Sicherheits-Profi! Unser SPAM-Filter, das Patch-Management und die super Reaktionszeiten sprechen doch eine klare Sprache. Wenn wir das noch mit dem neuen Datenschutzkonzept und der neuen Vereinzelungsanlage zum Forschungstrakt kombinieren, ist an der Überschrift nichts auszusetzen.“*

Auch Dave ist nicht wohl bei der Sache: *„Wir sollten uns lieber in Bescheidenheit üben, glaube ich. Meint ihr nicht, dass ein Artikel für die Mitarbeiter-Zeitung erst mal*

ausreicht? Das mit der Kunden-Info könnte man dem Chef ja vorschlagen, bezüglich der Dinge, die wir im nächsten Jahr noch verbessern wollen. Wenn ihm das gefällt, wäre das vielleicht ein Anreiz für mehr Rückendeckung und Bob wird den Titel als größter Arbeitsverhinderer los.“

| Gute Nachrichten:                                                                                                                                                                                                                                                                                                                                             | Medium:                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Einspielen von Updates</li> <li>- Bobs Security-Zertifikat</li> <li>- Anzahl gefilterter SPAM-Mails</li> <li>- Anzahl abgewiesener Port-Scans</li> <li>- Reaktionszeit auf Sicherheitsvorfälle</li> <li>- Möglichkeiten der Daten-Wiederherstellung</li> <li>- Vermeidung hoher Strafen durch Datenschutz</li> </ul> | <ul style="list-style-type: none"> <li>- Web-Portal</li> <li>- Info-Mail</li> <li>- Mitarbeiter-Zeitung</li> <li>- Plakate</li> <li>- Lokale Pressemitteilung</li> <li>- Kunden-Info</li> <li>- Vorstandspräsentation</li> </ul> |

**Abbildung 4-2:** Brainstorming der guten Nachrichten aus dem Sicherheitsteam

Alice, Bob und Dave einigen sich auf einen Artikel für die Mitarbeiter-Zeitung. Dem Vorstand wollen sie die bisherigen Erfolge präsentieren und vorschlagen, am Ende des Jahres mit den weiteren Verbesserungen in Form eines Informationsschreibens an die Kunden heranzutreten. Vielleicht haben sie Glück und er geht darauf ein.

Um auch in Zukunft mehr auf positive Nachrichten zu setzen, beschließen sie, sich ein Mal im Monat zu einem „Brainstorming der guten Nachrichten“ zu treffen, damit sie im alltäglichen Geschäft aus Bedrohungen, Risiken und Sicherheitsvorfällen nicht vergessen, über die Erfolge zu berichten.

#### 4.2.2 Negative Nachrichten meistern

Wenn der vorherige Abschnitt die Arbeit der Sicherheitsexperten aus der „Heile-Welt-Perspektive“ beleuchtet hat, so geht es nun darum, die unangenehmen Nachrichten in den Mittelpunkt der Betrachtung zu rücken. Vielleicht hat Sie beim vorherigen Abschnitt auch eine leise Skepsis beschlichen: Zum wahren Leben in der Security-Branche gehören nicht nur positive Nachrichten. Und man kommt sicher nicht zum Ziel, wenn man immer nur alles in den schillerndsten Farben beschreibt und sich ein Security-Wonderland zurechtlegt.

Alles Bitten und Betteln hilft nichts: Ein großer Teil der Security-Arbeit sind Gebote und Verbote und nicht jeder hält sich daran. Wie aber kommuniziert man sie, ohne im Verhaltenskreuz in Richtung Bevormundung und Geringschätzung

abzudriften? Wir haben bereits gesehen, dass diese Richtung schnurgerade in die Buhmann-Falle führt.

Die systemische Kommunikation bietet eine Möglichkeit, sich diesem Außenseiter-Problem aus einem weiteren Blickwinkel zu nähern.<sup>85</sup> Nach diesem Ansatz gibt es nicht auf der einen Seite einen Verursacher und auf der anderen Seite eine Wirkung, sondern immer eine bestimmte Wechselwirkung. Der Buhmann im Team ist also nicht der Verursacher und die Buh-Rufe des Teams nicht die Wirkung. Die Frage lautet: *„Was leistet der Buhmann innerhalb der Gesamtgruppe und was haben die Beteiligten davon, den Buhmann in seiner unangenehmen Rolle festzunageln?“* Die Gesamtgruppe wehrt sich instinktiv dagegen, dass der Buhmann eine wichtige Aufgabe für das Team leistet. Die Gruppenmitglieder finden es ganz angenehm, nicht selbst in die paranoide Welt aus Bedrohungen und Sicherheitsvorfällen eintauchen zu müssen. Diese Welt, in der man in Risiken und Sicherheitsmaßnahmen denkt, löst bei vielen Unbehagen aus. Sie würden sich lieber in einer Welt sehen, in der man unbekümmert alle Türen offen lassen kann. Wir haben dieses paradoxe Verhalten bereits im Abschnitt über den Vertrauensverlust durch Sicherheitsmaßnahmen betrachtet. Da kommt es gerade recht, das IT-Sicherheitsbeauftragte, Datenschützer und Co. diese unschöne Aufgabe übernehmen und man sich selbst auf die Position zurückziehen kann, von all diesen schlimmen Risiken nichts zu verstehen: Auch wenn die Sicherheitsprofis in der Buhmann-Falle festsitzen, so wissen doch alle auf eine verborgene Weise, dass sie für die Erhaltung des Gesamtsystems unentbehrlich sind.

In vielen Fällen übertreiben die Security-Buhmänner ihr Verhalten sogar und drängen sich damit selbst weiter in diese Rolle – unter Umständen gefallen sie sich sogar darin. Die Studie *„Aus der Abwehr in den Beichtstuhl“*<sup>86</sup> zitiert Sicherheitsprofis, denen es ähnlich geht. Dort wird konstatiert, dass ein guter Sicherheitsmann keine Freunde haben kann oder zumindest etwas nicht stimmt, wenn der CISO der beliebteste Mann im Unternehmen ist. Einer wird manchmal der Inquisitor genannt. Ich stand schon vor der Tür eines IT-Sicherheitsbeauftragten, an der das Bild Girolamo Savonarolas hing. Der war italienischer Dominikaner und Bußprediger und im 15. Jh. de facto Herrscher über Florenz. Er war für einige Hinrichtungen verantwortlich und sein Leben fand letztlich selbst bei einer Hinrichtung ein Ende.

Die Situation, dass das Gesamtkonzept davon abhängt, dass die Sicherheitsprofis in der Buhmann-Falle sitzen ist natürlich verheerend. Man legitimiert damit alle, die schlecht auf einen zu sprechen sind. Dies gilt es zu vermeiden, wenn negative

---

<sup>85</sup> Karl Benien; Schwierige Gespräche führen; 2007; rororo; ISBN 9783499614774; Seite 112 ff

<sup>86</sup> known\_sense (Herausgeber u.a.); Aus der Abwehr in den Beichtstuhl – Qualitative Wirkungsanalyse CISO & Co.; 2008; known\_sense; Seiten 12, 27, 28

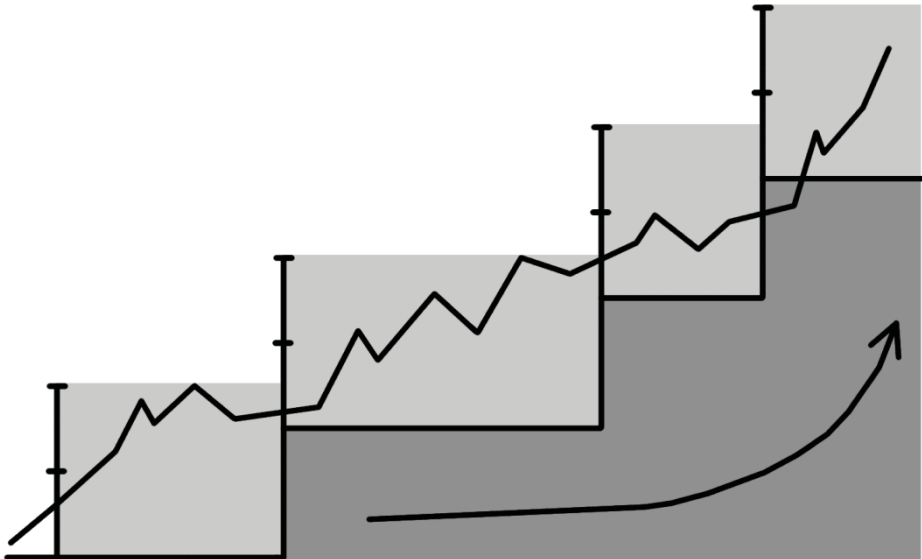
Nachrichten zu überbringen hat. Die negative Nachricht muss also zunächst einmal von der eigenen Person gelöst werden. Die Botschaft darf nicht sein, dass man nun mal fürs Überbringen der schlechten Nachrichten zuständig sei. Damit erfüllt man zwar das Rollenverständnis der Gruppe, die Botschaft bleibt jedoch auf der Strecke. Die typischen negativen Nachrichten der IT-Sicherheitsbeauftragten, Datenschützer und Co. sollten also von ihrer Sicherheitsrolle getrennt vorgebracht werden. Die nicht umgesetzten Maßnahmen sind nicht deshalb ein Problem, weil sie im Sicherheitskonzept stehen, sondern weil aus ihnen ein Risiko für die Ziele des Unternehmens oder der Behörde resultieren. Ein Sicherheitsvorfall ist kein Problem des Sicherheitsbeauftragten, sondern des Unternehmens.

Wer wie Alice, Bob und Dave im letzten Fallbeispiel vorgebaut und dafür gesorgt hat, dass Mitarbeiter und Chefs aus dem Sicherheitsteam auch mal positives zu hören bekommen, der wird bei der Überbringung schlechter Nachrichten überhaupt Gehör finden. Eine der Grundregeln guter Rhetorik zum Beispiel lautet, ab und an den Tonfall zu variieren. Wer will, dass das Publikum zuhört und sich nicht untereinander unterhält, der muss auch mal leiser sprechen. Wer immer leise spricht, dem schlafen die Zuhörer ein. Ein anderes Beispiel: Gute Chefs wissen, dass sich Lob und Tadel abwechseln müssen, damit sie noch wahrgenommen werden. Wenn es schon ein Lob ist, wenn der Chef mal zehn Minuten nicht schreit, dann ist das Gleichgewicht aus den Fugen geraten. Das gilt auch für Sicherheitsexperten: Die Balance macht den Erfolg. Wenn Sicherheitsexperten Schulnoten für Mitarbeiter und Chefs verteilen müssen, dürfen es nicht immer nur Fünfen und Sechsen sein!

Schlechte Nachrichten müssen immer im Verhältnis zu guten Nachrichten wahrgenommen werden können. Erst, wenn man dem Chef wochenlang erzählt hat, welche Erfolge man erzielen konnte, wird er wahrnehmen, wenn es plötzlich bergab geht. Gleiches gilt für die Mitarbeiter.

Der Empfänger macht die Nachricht. Es ist also im Sinne der Kommunikation nicht entscheidend, ob ein bestimmtes Verhalten objektiv gut oder schlecht ist, sondern subjektiv. Wenn man am Anfang einer verbesserten Sicherheitskultur steht, sind auch objektiv kleine Schritte schon ein subjektiver Erfolg. Vielleicht trivial: Was in der fünften Schulklasse in Mathematik für eine zwei reicht, reicht eben in der Abiturprüfung noch nicht mal für ein mitleidiges Lächeln des Prüfers. Und die besten Mathe-Noten reichen im Studium meist nicht mal übers erste Semester.

Schlechte Nachrichten müssen also nicht nur in einem angemessenen Verhältnis zu guten Nachrichten stehen, sondern auch zur konkreten subjektiven Situation passen.



**Abbildung 4-3:** Systematische Verschiebung der Y-Achse.

Was vor der der Versetzung in die nächste Klasse noch für gute Noten ausgereicht hat, entspricht nach der Versetzung nicht einmal dem Klassenziel (Abbildung 4-3). Auf diese Weise verschiebt sich die Bewertungs-Skala der Y-Achse systematisch nach oben. Da Unternehmen und Behörden nicht in Schuljahren funktionieren kann eine „Versetzung“ unter zwei Voraussetzungen angezeigt sein:

- ❖ Die intern gesetzten Ziele wurden erreicht – Zeit für neue Horizonte.
- ❖ Durch neue Bedrohungen, große Sicherheitsvorfälle oder andere externe Zwänge fällt die Notenskala objektiv so stark aus dem Rahmen, dass eine Anpassung nötig ist, auch wenn es schmerzhaft ist.

Aus den oben genannten Gründen ist es natürlich der Idealfall, wenn man sich den neuen Bewertungsmaßstab selbst auferlegen kann. Das ist aber nicht immer möglich. Manchmal sind die Sicherheitsbedenken größer, als die kommunikativen Zwänge: Dann muss es eben erst mal nur noch Sechsen geben und die Ergebnisse sind zunächst zwangsläufig „unterirdisch“.

#### 4.2.2.1 Fallbeispiel: Alles schrecklich in der ExAmple AG

In der ExAmple AG ist seit dem „Brainstorming der guten Nachrichten“ ein halbes Jahr vergangen. Alice, Bob und Dave hatten zuerst einen Artikel für die Mitarbeiter-Zeitung verfasst, in dem die Arbeit des Teams vorgestellt wurde: Die

für jeden eingesparte Arbeitszeit durch den SPAM-Filter, die täglich abgewehrten Port-Scans und die Reaktionszeit nach Sicherheitsvorfällen wurde darin in Form einer Reportage aufgearbeitet. Der Vorstand war nach einer Präsentation der bisherigen Erfolge damit einverstanden, am Ende des Jahres mit den weiteren Verbesserungen in Form eines Informationsschreibens an die Kunden heranzutreten. Gerade nach den Datenschutz-Skandalen der letzten Zeit hatte er ohnehin an so etwas gedacht. Seit dem arbeiten die drei regelmäßig mit der Marketing-Abteilung und der Unternehmenskommunikation zusammen. Im Verlauf der letzten Wochen hatte sich die Stimmung gegen Alice, Bob und Dave merklich aufgehellt und aus dem monatlichen „*Brainstorming der guten Nachrichten*“ konnten sie jede Menge Positives herausziehen und der Chef hatte sich schon bei einigen Kunden mit seinem tollen Sicherheitsteam gebrüstet.

Diese Woche jedoch stellte sich heraus, dass das Netzwerk der ExAmple AG durch Schadsoftware befallen ist. Auslöser waren einige Mitarbeiter, die untereinander ein Programm getauscht hatten, dass einen kleinen Nikolaus auf der Taskleiste umherwandern lässt. Leider war das nicht die einzige Funktion der `Nikolaus.exe` gewesen: Solange die Software läuft, schreibt sie jeden Tastaturanschlag mit und verschickt den Mitschnitt ein Mal in der Woche ins Internet. Das konnte Bob jedoch glücklicherweise vorher verhindern. Die Software hatte auch den Weg in die Forschungsabteilung gefunden und hätte dort schlimmen Schaden anrichten können. Bob ist skeptisch:

*„Der Virens Scanner hat den Trojaner gefunden und nicht ich – Kunststück.“*

Dave sieht das anders: *„Und wer betreibt den Virens Scanner? Wenn die Herren Forscher im Labor aus Versehen über das Jahrhundertmedikament stolpern, fragt auch keiner ob das ein Glücksfall war, für den sie dann den Nobelpreis bekommen. Ich kann mich noch genau erinnern, wie viel Arbeit du hattest, die Verteilung der Updates zuverlässig hinzubekommen. Wenn der Trojaner drei Tage später gefunden worden wäre, hätte es schon zu spät sein können.“*

*„Und genau das werden wir dem Chef berichten“, fügt Alice hinzu. „Jetzt haben wir ihn wochenlang mit guten Nachrichten Honig um den Mund geschmiert. Der geht bestimmt an die Decke, wenn er das hört. An uns kann es ja nicht gelegen haben.“*

Auch, wenn Bob eigentlich nicht für einen funktionierenden Virens Scanner gelobt werden will, stimmt er zu, auf den Chef zuzugehen: *„Müller, Meier, Schulz – Trojaner in die Forschungsabteilung angeschleppt: Sechs, setzen! Bei der Gelegenheit könnte man endlich vorschlagen, die Internet-Anbindung in die Forschungsabteilung zu unterbinden und das Netz stärker zu segmentieren. Man kann denen ja offensichtlich nicht über den Weg trauen.“*



**Abbildung 4-4:** Wohl dosiert zeigen Ermahnungen auch Wirkung

Mit Hilfe von Alice und Dave bereitet sich Bob auf den Termin beim Chef vor. Der ist natürlich überhaupt nicht begeistert und kann sich gar nicht erklären, wie es bloß so weit kommen konnte. Bob schildert ihm die Sache so:

*„Das hätte ganz schön ins Auge gehen können. Leider steht der Forschungs-Leiter nicht so richtig hinter der ganzen Security-Sache, obwohl es im Moment so super voran ging. Vielleicht war das für den einen oder anderen eine Einladung.“*

*„Wir waren doch auf einem so guten Weg“, sagt der Chef mit einigem Ärger. „Die schicken sich kleine Nikoläuse zu, weil sie keine Arbeit haben und dann ist Ihre ganze Arbeit dahin. So geht's nicht. Wir geben doch nicht zigtausend Euro für Sicherheitstechnik aus, damit die sich Nikoläuse zuschicken! Ich werde mir den Forschungs-Leiter mal vorknüpfen. Die sollen forschen und nicht rumspielen!“*

Jetzt kommt Bobs großer Moment: *„Ich denke, dass das erst mal nicht nötig ist. Ich schlage vor, dass ich noch mal mit ihm rede, und ihm die Schwierigkeiten erläutere, die durch so einen Fehler entstehen können. Wenn das auch nichts hilft können Sie ja auch noch mal mit ihm sprechen, aber ich denke, dass er es einsehen wird.“*

Der Chef geht auf Bobs Vorschlag ein und so hat Bob dem Abteilungsleiter nochmal den Kopf aus der Schlinge ziehen können, die er ihm zuvor vorsichtig um den Hals gelegt hatte. Gleichzeitig hat er sich so eine weitere Eskalationsstufe geschaffen, mit der er in Zukunft drohen kann.

## 4.3 Security-Storyboard

Im Kapitel über die Security-Bühne haben wir die historischen Beispiele von Pawero im alten Ägypten und von General Meng-tian aus den Zeiten des Kaisers Qin Shiuangdi kennengelernt: Wenn ein Schutzwall seit längerer Zeit seinen Zweck erfüllt, wird in Frage gestellt, was die ganzen Anstrengungen bringen sollen. Und fast immer lässt sich ein Phasenverlauf ablesen, nach dem auf der klassischen Security-Bühne gespielt wird. Der erste Akt heißt *Panik*, der zweite Akt *Rückfall*. Die Handlung geht aus der *Naivität* über einen *Vorfall* zurück in die *Naivität*. Security ist durch Vorfälle gesteuert, nach denen Maßnahmen ergriffen werden, die dafür sorgen, dass es keine Vorfälle mehr gibt. Entlang dieser Wellenbewegung verläuft das Security-Storyboard.

|                          |              |               |             |
|--------------------------|--------------|---------------|-------------|
| <b>1. Akt „Panik“</b>    | 1. Naivität  | 2. Vorfall    | 3. Angst    |
| <b>2. Akt „Rückfall“</b> | 4. Maßnahmen | 5. Beruhigung | 6. Naivität |

**Tabelle 4-4:** Das Security-Storyboard mit seinen sechs Szenen

Die meisten Sicherheitsbeauftragten hängen in der 6. Szene fest und legen nur ab und an eine Schleife über die Szenen 2. bis 5. ein. Dabei geben sich alle Beteiligten große Mühe, in Windeseile zur 6. Szene zurückzukehren. Im Verlauf dieser Wellenbewegung ändern sich vor allem die äußeren Zwänge, die auf IT-Sicherheitsbeauftragte, Datenschützer und Co. einwirken. Sind die Beteiligten von Angst ergriffen, wird nach harten Maßnahmen gerufen. Gerät der Vorfall in Vergessenheit, kehrt sich der Ruf nach Maßnahmen ins Gegenteil. In der 4. Szene des Security-Storyboards haben Sicherheitsexperten ihre besten Momente. Wir wollen nun die Szenen noch einmal genauer betrachten und überlegen, wie man den Verlauf in der Praxis beeinflussen kann, damit Mitarbeiter und Chefs nicht immer wieder zurück in die Naivität verfallen. Unser Ziel lautet: So schnell wie möglich in die 4. Szene!

### 4.3.1 Erster Akt: Panik

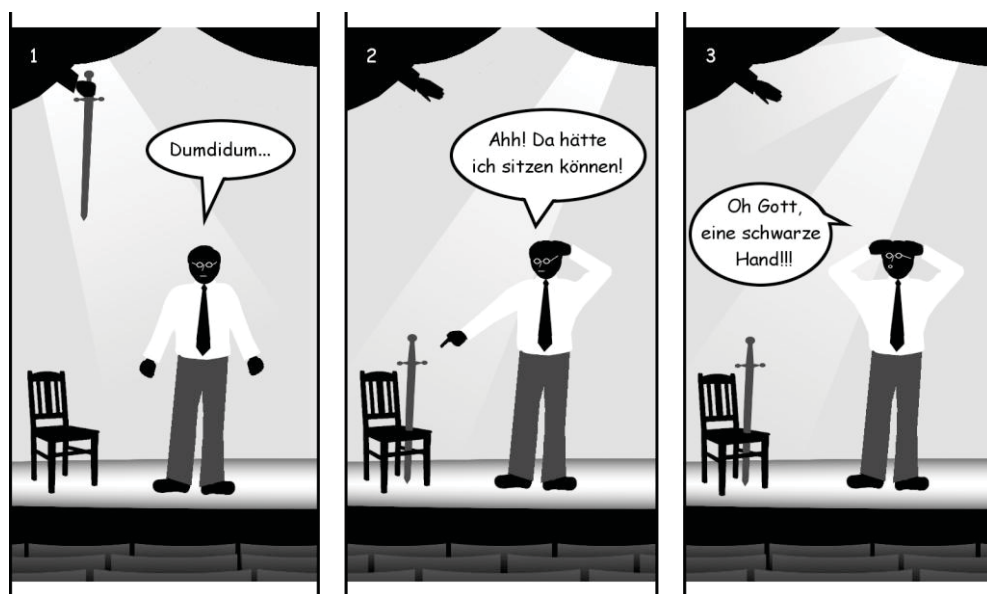
In der ersten Szene ist die drohende Gefahr noch unbekannt und keiner der Akteure rechnet mit etwas Schlimmem. Unternehmen oder Behörden, die sich in diesem frühen Stadium des Security-Storyboards befinden, erinnern an den Beginn der Fälle in Aktenzeichen XY oder die ersten zehn Minuten in Horrorfilmen und die Zuschauer schlüpfen in die Rolle der Security-Experten: Durch die Filmtitel aufgestachelt, rechnen sie mit dem Schlimmsten. Heißt der Film ‚Der Tod aus der Dunkelheit‘, warnt die innere Stimme: „*Nein, nicht in den dunklen Keller gehen.*“ Und

wenn bei Aktenzeichen XY Frau Schröder abends das Fenster kippt ist klar: „*Das war ihr letztes gekipptes Fenster.*“

Ebenso hilflos, wie die Zuschauer das unvermeidliche kommen sehen und nichts machen können, sind auch die Security-Experten hilflos, wenn ihre Chefs und Mitarbeiter in der ersten Szene festhängen.

Um die Akteure aus dem Dornröschenschlaf zu wecken hilft nur eins: Ein Vorfall oder eine Awareness-Kampagne! Wie die Akteure in der zweiten Szene wacherüttelt werden, ist für den Verlauf der Handlung nicht so wichtig – möglichst glaubhaft muss es sein, damit der erste Akt in der allgemeinen Panik der Beteiligten seinen Höhepunkt finden kann.

In der dritten Szene macht sich die Angst breit, dass man von Anfang an viel zu naiv war. Nach dem ersten Schock steht fest: Das Erlebte bzw. Vorgeführte kann sich jederzeit wiederholen. Den Beteiligten wird klar, dass sie dieser Gefahr ohne die Hilfe eines Experten schutzlos ausgeliefert sind: Der erste Akt ist vorüber.



**Abbildung 4-5:** Erster Akt: 1. Naivität, 2. Vorfall, 3. Angst

Für IT-Sicherheitsbeauftragte, Datenschützer und Co. muss klar sein: Der erste Akt muss im Schnelldurchlauf abgehakt werden. Dazu müssen insbesondere Naivität und Unwissenheit in Bezug auf Sicherheitsvorfälle bekämpft werden. Je eindringlicher die drohenden Gefahren aufgezeigt werden, je eindringlicher wird deren Beseitigung gefordert werden. Dabei sollte nicht vergessen werden, die Gefahren in die Problemfelder der Chefs und Mitarbeiter zu übersetzen: Zwänge,

Ziele, Prioritäten und Risiken – Entscheidend sind die Problemfelder der Betroffenen, nicht die des Sicherheitsteams.

### 4.3.2 Zweiter Akt: Rückfall

Der erste Akt endete mit Angst, Ratlosigkeit und dem Ruf nach den Sicherheitsexperten. In der vierten Szene können nun die Maßnahmen zur Gefahrenabwehr ohne Widerstand vorgestellt und umgesetzt werden. Alle sind froh, aus der Not gerettet zu werden. Je besser die zweite Szene auf die Problemfelder der Chefs und Mitarbeiter zugeschnitten war, umso mehr kann jetzt erreicht werden. Das Problem, das diese Szene aus Sicherheitssicht mit sich bringt, besteht darin, dass durch die Sicherheitsmaßnahmen die gerade eben erst mühsam aufgebaute Drohkulisse Stück für Stück in sich zusammenbröckelt. In gewisser Weise zerstören Sicherheitsbeauftragte dadurch ihre eigene Arbeit. An dieser Stelle der Handlung gleitet man unweigerlich und sanft in die fünfte Szene.

In Hollywood-Filmen ist die fünfte Szene des Security-Storyboards die Schluss-Szene<sup>87</sup>. Sie ist ja auch die schönste – alle sind zufrieden. In der Realität der Security-Bühne sieht es anders aus und die Sicherheitsexperten wissen das: Die Leute in Horror-Filmen gehen immer wieder in dunkle Keller und Frau Schröders kippen seit 1967<sup>88</sup> nachts ihre Fenster und werden das leider auch in Zukunft tun. Die eigentliche Aufgabe ist es, bei neuen Bedrohungen von der fünften Szene direkt wieder ohne Umschweife in die vierte zurück zu kommen. Der schlechteste Fall wäre es, im Rahmen der sechsten Szene wieder in den alten, naiven Trott zurückzufallen.

Die sechste Szene findet man in Hollywood-Filmen meist als Beginn des zweiten Teils. Zum Beispiel in *Alien I-IV*<sup>89</sup> – Obwohl sich alle sicher waren: Das Alien war immer zu Beginn des nächsten Teils doch nicht tot. Nur die Hauptdarstellerin Lt. Ellen Ripley hat immer gewusst, dass die Gefahr weiterhin besteht. Ripley unterliegt übrigens im zweiten Teil der Sage demselben Irrglauben, dem auch manche Sicherheitsexperten unterliegen: Sie geht davon aus, dass man ihr für die Beseitigung des Aliens danken wird – Fehlanzeige. Ihr wird sogar die Fluglizenz entzogen.

Der Zyklus von der Naivität über Bedrohungen, Vorfälle und Maßnahmen zurück zur Naivität, scheint dem Security-Storyboard fest vorgegeben, die Dramaturgie

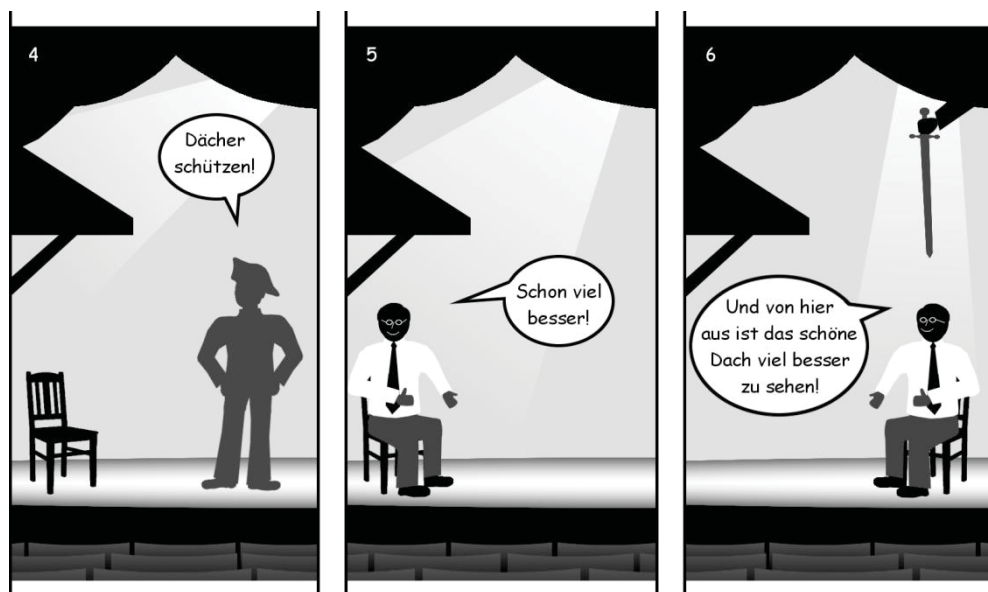
---

<sup>87</sup> Manchmal werden aus dramaturgischen Gründen die Szenen 2 – 5 noch einmal im Schnelldurchlauf wiederholt. Zum Beispiel ist der falsche Täter inhaftiert worden und der richtige mordet weiter.

<sup>88</sup> Eduard Zimmermann startete die Sendung Aktenzeichen XY am 20. Oktober 1967.

<sup>89</sup> *Alien – Die Saga*; Twentieth Century Fox Home Entertainment LLC

unausweichlich. Auch das notwendige Wechselspiel von guten und schlechten Nachrichten, dass wir im letzten Abschnitt betrachtet haben scheint diesen Zyklus nachzuzeichnen. Wir haben aber bereits da gesehen, dass wir der Handlung nicht hilflos ausgeliefert sind, sondern sie bewusst beeinflussen können. Wenn man das nicht tut, schrumpft die schöne Zeit der vierten Szene schlimmstenfalls auf wenige Tage im Jahr zusammen. Der Rest des Jahres spielt dann fast vollständig in den wenig erbaulichen Szenen eins und sechs.



**Abbildung 4-6:** Zweiter Akt: 4. Maßnahmen, 5. Beruhigung, 6. Naivität

Man muss sich also regelmäßig fragen, wo man mit dem eigenen Unternehmen oder der Behörde gerade steht. In Verbindung mit den Vorschlägen aus dem Abschnitt über gute und schlechte Nachrichten bedeutet das, dass die vierte und fünfte Szene die Zeit der guten Nachrichten umfasst und die sechste Szene in Form von schlechten Nachrichten vorweg genommen werden muss. Wenn man nicht permanent und über das ganze Jahr hinweg den Teufel an die Wand malt, bekommt man sogar mit hoher Wahrscheinlichkeit Gehör geschenkt.

Vor allem sollten Sie von den Betroffenen nicht zu viel Verständnis für die Funktionsweise von Sicherheitsmaßnahmen erwarten (Abbildung 4-6 versucht das anzudeuten). Mir hat kürzlich ein Bekannter mit seinem Blackberry Smartphone aus einem Flugzeug eine E-Mail geschickt, weil dort das Einschalten des Telefons aus Sicherheitsgründen verboten sei. Dass die E-Mail natürlich über das Telefonnetz übertragen wurde, war ihm weder bekannt noch irgendwie verständlich zu machen.

## 4.4 Security braucht Avatare

Avatare kennt man vor allem aus dem Internet, als grafischer Stellvertreter einer echten Person in einer virtuellen Welt. Aber auch im Rahmen von e-Learning-Programmen oder im Marketing werden Avatare eingesetzt, um Kommunikationsprozesse zu verbessern. Auch in Internetforen werden Avatare genutzt, um die Nutzer mit dem Bild einer virtuellen Person zu identifizieren. Das Wort kommt aus dem Hinduismus und bezieht sich auf das Herabsteigen einer Gottheit in irdische Sphären.<sup>90</sup> Avatare existieren in Form eines Bildes, eines Icons oder sogar als animierte 3D-Figur. Die heutige Bedeutung des Begriffs geht auf den Roman *Snow Crash*<sup>91</sup> zurück.

Wenn man Avatare als graphische Stellvertreter bezeichnet, dann gibt es diese nicht erst seit diesem Jahrhundert. Auch vorher wurden graphische Stellvertreter eingesetzt, um bestimmte Eigenschaften und Botschaften zu transportieren. So wurde das HB-Männchen aus der bekannten Zigarettenwerbung der 60er Jahre zum Avatar für die Marke HB der British American Tobacco. Das HB-Männchen durfte machen was es wollte, man mochte es einfach. Ausgangspunkt waren verschiedene Alltags-Szenen, in denen irgendetwas schief ging, worüber sich das HB-Männchen Bruno gehörig aufregte. Die Aufregung steigerte sich so sehr, bis das HB-Männchen buchstäblich in die Luft ging.

*„Halt! Wer wird denn gleich in die Luft gehen? Greife lieber zu HB. Dann geht alles wie von selbst.“*

Und Bruno schwebte wieder zurück auf den Boden.<sup>92</sup> Auch heute noch geht man *„in die Luft, wie ein HB-Männchen“*.

*„Also eigentlich ist das kleine HB-Männchen aus der Security Abteilung ja ganz knuffig“,* sagt die eine Mitarbeiterin zur anderen.

Was liegt also näher, als sich damit auseinander zu setzen, wie man ähnliche Methoden auch für das Marketing von Sicherheit verwenden kann. Das positive Endergebnis aus der eher unangenehmen Alltagssituation wird dabei mit dem

---

<sup>90</sup> Alycia de Mesa; *Brand Avatar: Translating Virtual World Branding Into Real World Success*; 2009; Palgrave Macmillan; ISBN: 9780230201798; Seite 173 ➤

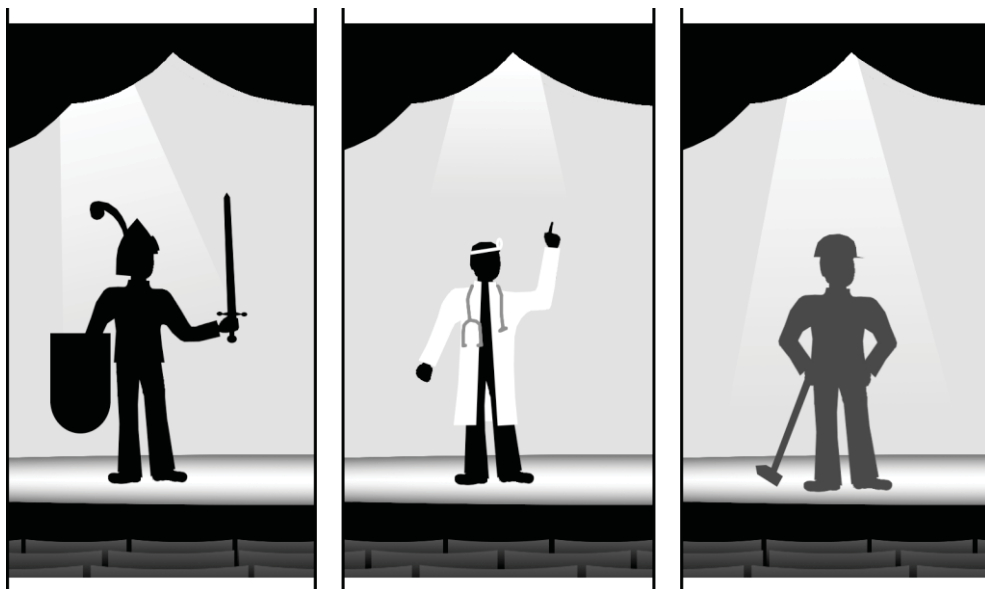
<sup>91</sup> Neal Stephenson; *Snow Crash*; 2000; Spectra; ISBN 978-0553380958

<sup>92</sup> Roman Anlanger; *Trojanisches Marketing: Mit unkonventioneller Werbung zum Markterfolg*; 2009; Rudolf Haufe Verlag; ISBN: 9783448087208; Seite 118 ➤

Produkt in Verbindung gebracht. Ein ähnliches Konzept verfolgt die Werbung mit den beflügelten Zeichentrickfiguren von Red-Bull.

Die Gestaltung eines Avatars ist dabei durchaus leichter als man denkt – es gibt unzählige Vorlagen: Denken Sie an Märchen, Sagen oder die griechische Mythologie. Die dort enthaltenen Figuren sind oft schon seit der Kindheit bekannt und sie alle werden mit einer bestimmten Aussage verknüpft, auf der man aufbauen kann. So gibt es in Köln einen Security-Stammtisch, der unter der Headline *„Wölfe und Geißen“*<sup>93</sup> auftritt. Für jeden, der das Märchen *„Der Wolf und die sieben Geißlein“* kennt, transportiert diese Bezeichnung eine gewisse Vorstellung davon, um was es dort geht, und das deutlich besser, wie es die Bezeichnung *„Security-Stammtisch“* vermag.

Aber nicht nur Märchen oder Geschichten kommen in Frage, um der Kommunikation auf die Sprünge zu helfen. Auch Gegenstände oder Gesten können dazu benutzt werden, gewisse Assoziationen hervorzurufen. Das gilt immer dann, wenn diese quasi als Aushängeschild einer gewissen Botschaft dienen. Denken Sie zum Beispiel an einen weißen Kittel: Wissenschaftliche Seriosität. Oder raufgekremelte Ärmel: Keine Theorie – Praxis. Oder die flache Hand auf die Stirn: Fehler oder Vergessen. Die Liste ließe sich beliebig fortsetzen.



**Abbildung 4-7:** Unterschiedliche Avatare rufen unterschiedliche Assoziationen hervor.

<sup>93</sup> <http://www.woelfegeissen.de>

Entscheidend dabei ist, welche Botschaft man präsentiert, und welche Zielgruppe man erreichen will. Die Geschichte, der Gegenstand oder die Geste müssen innerhalb der Zielgruppe funktionieren. Das bedeutet natürlich, dass es nicht den einen Avatar gibt, mit dem man immer erfolgreich ist. Ohne eine individuelle Zielgruppenanalyse kann man schnell daneben liegen. Die gescheiterte Kampagne bleibt dann übrigens aus den gerade geschilderten Gründen ebenso erfolgreich im Gedächtnis. Es ist also Vorsicht geboten und man sollte bei der Umsetzung eine externe Beratung durchaus in Erwägung ziehen.

Die Aufgabe des Security-Avatars als graphischer Stellvertreter ist es, auf der einen Seite, die Person aus der realen Welt mit bestimmten zusätzlichen Eigenschaften auszustatten. Auf der anderen Seite soll dem Avatar eine bestimmte Botschaft anhaften, die übermittelt werden soll. Bei der Ideensammlung für einen geeigneten Avatar müssen die drei folgenden Fragen berücksichtigt und mit „ja“ beantwortet werden:

- ❖ Passt der Avatar zur Botschaft?
- ❖ Passt der Avatar zur Zielgruppe?
- ❖ Passt der Avatar zu seinem realen Gegenstück

Wir wollen uns diesen Fragen im folgenden Abschnitt annähern. Die Frage nach der Zielgruppe ist darüberhinaus immer auch individuell und auf den Einzelfall bezogen zu beantworten.

Was ist also die Botschaft der IT-Sicherheitsbeauftragten, der Datenschützer und Co? Sie verkaufen Sicherheit und ihre Botschaft lautet: *„Geht keine unnötigen Risiken ein. Seid wachsam. Hütet euch vor Fremden.“* Die Frage, ob der Avatar zur Botschaft passt muss auf dieser Grundlage beantwortet werden. Auch hier kann es im konkreten Einzelfall Varianten der Botschaft geben, die zu berücksichtigen wären. Um festzustellen, ob ein Avatar zu den Botschaften der Security-Experten passt, empfiehlt sich als erster Anhaltspunkt eine Matrix, in der die Botschaften und die Ideen für Avatare gegenübergestellt werden:

| Botschaften/ Avatare                       | Ritter | Arzt | Bauarbeiter |
|--------------------------------------------|--------|------|-------------|
| <i>„Geht keine unnötigen Risiken ein!“</i> | +/-    | ++   | +/-         |
| <i>„Seid wachsam!“</i>                     | ++     | +    | +/-         |
| <i>„Hütet euch vor Fremden!“</i>           | +      | -    | +/-         |

**Tabelle 4-5:** Beispiel-Matrix zur Bewertung der Ideen für Avatare

Diese Matrix sollte aber nicht alleine entscheidungsrelevant sein. Auch wenn der Bauarbeiter in der Beispieltabelle eher schlecht abschneidet, kann er für eine besondere Zielgruppe – zum Beispiel die Mitarbeiter einer Bauunternehmung – die erste Wahl sein. Je nach Zielgruppe können auch Avatare erfolgreich sein, die für die Botschaft kaum geeignet oder sogar konträr zur Botschaft sind und dadurch einen besonderen Kontrast setzen. Denken Sie beispielsweise an die Fernseh-Werbung, in der ein Rocker fürs Bausparen wirbt. Auch wenn dieses Beispiel nur bedingt geeignet ist, weil der Rocker ja den Kunden darstellt und nicht den Anbieter, so zeigt es doch: Erlaubt ist, was für die Zielgruppe funktioniert. Daher sind die Ergebnisse der Matrix auch nur ein erster Anhalt. Man sollte durchaus versuchen, sie mit anderen Argumenten zur Zielgruppe weiterzuentwickeln.

Zuletzt sollte der gewählte Avatar auch zu seinem Gegenstück aus der realen Welt passen und diesen möglichst nicht karikieren. Wenn das virtuelle Konterfei der nächsten Awareness-Kampagne, den Spott über das betroffene Security-Team anregt, dann ist es sicher nicht geeignet, die Sicherheit im Unternehmen oder der Behörde voranzutreiben.

#### 4.4.1 Fallbeispiel: Herkules und der Stall des Augias

Herkules ist ein Halbgott in der griechischen Mythologie. Ihm wurden vom König Eurystheus zwölf Aufgaben gestellt, die er zu bewältigen hatte, um sich von dem im Wahnsinn verübten Mord an seiner Frau Megara und seinen mit ihr gezeugten drei Söhnen rein zu waschen. Eine der zwölf Aufgaben bestand darin, die Rinderställe des Augias auszumisten. Diese unwürdige Aufgabe war für einen Helden nicht nur herabwürdigend, sondern selbst für Herkules nahezu unerfüllbar. Die Ställe des Augias waren schon seit 30 Jahren nicht mehr ausgemistet worden und das bei der stattlichen Anzahl von über 3.000 Rindern. Eurystheus wollte zudem, dass Herkules die Aufgabe binnen eines Tages lösen sollte.

Noch heute werden stark verdreckte Räume als Augias-Ställe bezeichnet. Die Redewendung, *„einen Augias-Stall ausmisten“*, bedeutet so viel wie *„gründlich aufräumen“*. Der Augias-Stall ist unter den verdeckten Ställen dieser Welt der größte. Herkules löste die Aufgabe, indem er das Wasser der Flüsse Alpheios und Peneios durch den Stall leitete. Herkules scheint also gut geeignet als Avatar für die Security-Bühne. Das haben sich auch der IT-Sicherheitsbeauftragte Bob, die Datenschutzbeauftragte Alice und der Sicherheitsbeauftragte Dave aus der ExAmple AG gedacht: *„Ein Mal den ganzen Laden so richtig durchspülen – das wär’s!“*

Die drei Sicherheitsexperten unseres Pharma-Unternehmens wollen der Security-Offensive, die sie für das nächste Jahr geplant haben, ein Gesicht geben. Ein Avatar soll Pate stehen und die Botschaft transportieren. Herkules scheint ihnen für die

Botschaft wie geschaffen. Gleich morgen wollen sie die Kampagne entwerfen und so schnell wie möglich in die Tat umsetzen.

Am nächsten Morgen machen sie sich ans Werk und Bob erfasst in einer Tabelle einige Botschaften, die er dann mit Herkules in Verbindung bringt: *„Der Chef hat uns aufgetragen, den Security-Dreckstall ExAmple AG auszumisten – wegen der Übermacht der „Rindviecher“ eine fast unlösbare Aufgabe.“*

Schnell sind die Botschaften in eine Tabelle eingetragen, die zeigt, dass die drei goldrichtig liegen (Tabelle 4-6). Herkules ist genau der richtige Mann für ihr Projekt.

| Botschaften/ Avatar                    | Herkules |
|----------------------------------------|----------|
| <i>„Saustall ausmisten.“</i>           | +++      |
| <i>„Fast unlösbare Aufgabe...“</i>     | +++      |
| <i>„... die trotzdem gelöst wird.“</i> | +++      |
| <i>„Vom Chef aufgelegt.“</i>           | +++      |
| <i>„3000 Rinder machen Mist.“</i>      | +++      |

**Tabelle 4-6:** Alice, Bob und Dave entscheiden sich für Herkules

Herkules wird das Gesicht der kommenden Security-Offensive: Er schmückt Plakate, Flyer und er steht lebensgroß im Foyer. Eine Sprechblase verkündet: *„Jetzt wird mal so richtig ausgemistet – Schluss mit unsicher!“* Er wird das Maskottchen der neuen Datenschutz-e-Learning-Plattform und unter seinem Namen erscheint zum ersten Mal eine Security-Kolumne in der Mitarbeiterzeitung. Alice, Bob und Dave sind mit ihrem Avatar sehr zufrieden. Sie freuen sich, so schnell zu Ergebnissen gekommen zu sein.

Nach wenigen Tagen melden sich die ersten Mitarbeiter mit kritischen Bemerkungen zu Wort. Ein Chemiker aus der Forschung sagt: *„Ihr seid also die Helden und wir die 3000 Rinder?! Das erkennt man ja gleich, wie ihr tickt.“* Eine Mitarbeiterin aus der Personalabteilung fragt: *„Ihr seid wohl eher Augias als Herkules! Wer hat es denn so weit kommen lassen?“* Und der Controller stellt resigniert fest: *„Und dafür ist also Geld da!“* Der Betriebsrat hatte von der ganzen Aktion nichts mitbekommen und ist sauer. Es dauert nicht lange, bis er die Sache aufgreift und mit dem Vorstand einen Termin vereinbart: *„Wir lassen nicht zu, dass wir hier wie die Rinder in Augias' Stall dargestellt werden, nur weil wir unsere Arbeit machen. Wenn der Stall verdreckt ist, hat der Stallbursche versagt.“* Der Vorstand kommentiert: *„Ich sag es*

ja immer: Die größten Arbeitsverhinderer! Bob, der IT-SiBe, ist der schlimmste! Am besten, wir setzen ihn auf die Straße.“

In diesem Moment wacht Bob schweißnass in seinem Bett auf – dass alles so furchtbar schief ging, hatte er nur geträumt. Gestern hatten er und seine beiden Kollegen Alice und Dave die Idee, dass Herkules der richtige Mann für die geplante Security-Offensive sei. In der Arbeit angekommen, setzt er sich sofort mit Alice und Dave zusammen, um zu verhindern, dass der Albtraum der vergangenen Nacht Wirklichkeit werden könnte.

Wir wollen uns nun anhand von Bobs Albtraum systematisch überlegen, welche Fehler zu dem Fiasko geführt haben könnten. Wir greifen hierfür zurück an den Anfang des Buchs, als wir uns auf Seite 8 mit den vier Problemfeldern Zwänge, Ziele, Prioritäten und Risiken auseinandergesetzt haben. Wir hatten dort als Qualitätskriterium einer Nachricht festgehalten, dass diese subjektiv für den Empfänger innerhalb seiner Problemfelder verständlich sein muss. Bobs Irrweg begann mit der Botschaft, die er übermitteln wollte: *„Der Chef hat uns aufgetragen, den Security-Saustall ExAmple AG auszumisten – wegen der Übermacht der „Rindviecher“ eine fast unlösbare Aufgabe.“* Diese Botschaft ist vielleicht auf die vier Problemfelder von Alice, Bob und Dave zugeschnitten – in keinem Fall jedoch auf die Mitarbeiter.

| Problemfelder:<br>Botschaften:  | Zwänge |    | Zeile |    | Priorität. |    | Risiken |    |
|---------------------------------|--------|----|-------|----|------------|----|---------|----|
|                                 | M      | S  | M     | S  | M          | S  | M       | S  |
| „Saustall ausmisten.“           | +      | ++ | -     | ++ | -          | ++ | -       | -  |
| „Fast unlösbare Aufgabe...“     | -      | -  | -     | -  | -          | -  | -       | ++ |
| „... die trotzdem gelöst wird.“ | +      | -  | -     | ++ | -          | ++ | -       | -  |
| „Vom Chef auferlegt.“           | -      | ++ | -     | -  | -          | -  | +       | -  |
| „3000 Rinder machen Mist.“      | -      | -  | -     | -  | -          | -  | -       | ++ |

**Tabelle 4-7:** Werden die Problemfelder richtig angesprochen?  
(M = Mitarbeiter; S = Security-Team)

In Tabelle 4-7 erkennt man schnell, dass die ausgewählten Botschaften nur in den Problemfeldern des Security-Teams punkten können. Für die Mitarbeiter stellen sie bestenfalls Zwang und Risiko dar: Keine gute Mischung, um sie zu überzeugen. Die Auswahl der Botschaft führt in der Folge dazu, dass man den Sympathie tragenden Helden schnell mit den Security-Experten verbindet: Für die Mitarbeiter bleiben dann nur noch die Rindviecher – nicht besonders wertschätzend. Das

Wortbild „Saustall ausmisten“ lässt zusätzlich wenig Spielraum für Entscheidungsfreiheit der Betroffenen. Dadurch driftet die Kampagne im Verhaltenskreuz nach Schulz von Thun (siehe Seite 44) in den ungünstigsten der vier Sektoren ab. Zuletzt zieht dann der vorschnelle Alleingang den Unmut des Betriebsrats auf sich, weil er von der ganzen Sache nichts gewusst hat – unnötig. (Siehe Abschnitt 1.4 Personal- und Interessenvertretungen)

Ist Herkules deshalb als Held der Kampagne ungeeignet? Keinesfalls. Wenn die Figur im Vorfeld so positioniert wird, dass die Mitarbeiter in der Figur ihre Problemfelder wiederfinden und die Kampagne mit allen Beteiligten gemeinsam angegangen wird, dann kann der Charme eines mythologischen Helden durchaus gute Dienste in der Kampagne leisten.



**Abbildung 4-8:** Stallbursche, Rind oder Papp-Herkules – wer ist hier wer?

Das erste, was Bob und seine beiden Kollegen machen müssen: Andere mit ins Boot holen. Wenn sie hinter die Zwänge, Ziele, Prioritäten und Risiken der Mitarbeiter kommen wollen, auf die sie dann die zu übermittelnde Botschaft abstimmen müssen, dann sollten sie mit ihnen sprechen. Aber nicht nur die Mitarbeiter sind wichtig. Für die Sicherheitsexperten schlägt das Risiko zu Buche, sich mit Interessenvertretungen und dem Vorstand Ärger einzuhandeln. Daher müssen sie auch hier die Kommunikation verstärken. Am besten ist es natürlich, wenn man das Gespräch in eine Richtung lenken kann, aus der die Gesprächspartner die Idee der Sicherheitsexperten so wahrnehmen, als sei es die eigene gewesen.

## 4.5 Security ist Cool

Aus irgendeinem Grund stecken viele Sicherheitsexperten nicht nur in der Buhmann-Falle fest, sondern gelten obendrein als ausgesprochen uncoole, spießige Bedenkenträger, die immer alles schwarz sehen und hinter jedem Menschen einen potentiellen Kriminellen sehen – alles ziemlich uncool. Ein Klischee, das verwundert, wenn man sich das Image von „Sicherheitsexperten“ aus dem Kino anschaut.

„Duplicity“ ist eigentlich ein Thriller, der aber das Zeug zum Social Engineering Lehrfilm hat. In Tony Gilroys Film jagen Julia Roberts und Clive Owen einem Produkt hinterher, von dem niemand weiß, was es eigentlich ist. Jedenfalls ist es sehr viel Geld wert. Die beiden ehemaligen Agenten – sie beim CIA, er beim MI6 – setzen ihre Kenntnisse mittlerweile als Sicherheitsberater und Industrie-Spione ein und versuchen ihre Auftraggeber gegeneinander auszuspielen. Dabei kommen eine ganze Reihe Social Engineering Techniken zum Einsatz. Zum Beispiel die Verführung der schüchternen Angestellten aus der Reisestelle. Die wird von ihrem Romeo-Agenten Clive Owen derart gut „geködert“, dass sie selbst nachdem sie aufgefliegen ist, immer noch ekstatisch zu Protokoll gibt, dass sie es jederzeit wieder tun würde. Die Anbahnungsszene bereichert jede Security-Schulung!

| Jahr | Titel <sup>94</sup>      | Handlung                                                                                                                                                                                                                                  |
|------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1973 | Der Clou                 | Schwerpunkt sind Trickbetrügereien. Aus Sicht der Information Security besonders interessant: Das Vortäuschen einer Radiosendung als Man-in-the-middle-Attacke.                                                                           |
| 1975 | Die drei Tage des Condor | Robert Redford spielt einen verfolgten CIA-Agenten, der Fernmeldetechniker beim Militär war. Interessant: Durch sein Insider-Wissen erhält er von der Telefongesellschaft Name und Adresse der Person hinter einer Telefonnummer genannt. |
| 1992 | Sneakers - Die Lautlosen | Spionagefilm, der sich um einen geheimen Krypto-Chip dreht. U.a. werden auch Bankkonten manipuliert und das Geld an gemeinnützige Organisationen verschoben.                                                                              |

**Tabelle 4-8:** Filmliste zu Security-Themen (Fortsetzung nächste Seite)

<sup>94</sup> *Der Clou* (a), *Die drei Tage des Condor* (b), *Sneakers* (c) und *Insider* (d) in Kevin Mitnick; Die Kunst der Täuschung; 2003; mitp; ISBN: 978-3-8266-1569-6; Seite 159 (a), 102 (b), 255 (c), 261 (d)

|      |                                   |                                                                                                                                                                                                                                    |
|------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1998 | 23 - Nichts ist so wie es scheint | Nach wahren Begebenheiten. Hier wird gehackt und spioniert was das Zeug hält. Im Mittelpunkt: Das Leben des Chaos-Computer-Club-Mitglieds Karl Koch <sup>95</sup> und dessen mysteriöser Tod.                                      |
| 1999 | Insider                           | Ebenfalls nach einer wahren Begebenheit. Im Mittelpunkt steht ein Insider der Tabakindustrie, der sein brisantes Wissen mit der Presse „teilt“.                                                                                    |
| 2000 | Takedown                          | Film über Kevin Mitnick. Im Mittelpunkt Hacking, Viren und Social Engineering.                                                                                                                                                     |
| 2002 | Spurwechsel                       | Ben Affleck verliert in dem Film bei einem Auto-Unfall eine Akte mit dem letzten Willen eines Multimillionärs. In der Folge kommt es zu Erpressung, Urkundenfälschung und der Manipulation von Bankkonten durch einen Hacker.      |
| 2002 | Catch me if you can               | Auch in diesem Film wird die Realität zitiert: Es geht um die Begebenheiten im Leben des Frank W. Abagnale – Betrügereien, Fälschungen und Social Engineering am laufenden Band.                                                   |
| 2007 | Stirb langsam 4.0                 | Ein in Ungnade gefallener Pentagon-Sicherheitsexperte bringt alle Computernetzwerke des Landes unter seine Kontrolle. Natürlich gelingt es Bruce Willis auch diesmal – wenn auch mit der Hilfe zweier Hacker – die Welt zu retten. |
| 2008 | Burn After Reading                | Spionagekomödie, die sich u.a. um brisante Informationen auf einer CD dreht, die in einer Umkleidekabine eines Fitness-Studios liegen geblieben ist.                                                                               |
| 2009 | Duplicity                         | Zwei Ex-Agenten setzen ihre Kenntnisse wechselnd als Sicherheitsberater und Industrie-Spione ein und versuchen ihre Auftraggeber gegeneinander auszuspielen.                                                                       |

**Tabelle 4-8:** Filmliste zu Security-Themen

<sup>95</sup> Mehr Informationen in „23 – Der Pressespiegel zu den realen Geschehnissen“, <http://www.uni-muenster.de/PeaCon/conspiracy/film23/Presse.htm>; eingesehen am 21.11.2009

Den Protagonisten aus Security-Filmen haftet eine gewisse Coolness an. Warum gelingt es so wenigen Sicherheitsexperten dieses Image auf sich zu übertragen. Dies wäre schon in Sachen Eigenmotivation ein wichtiger Schritt und es lohnt sich auch, dieses positive Image nach außen hin zu kommunizieren. Auch die Avatare aus dem vorherigen Abschnitt sind dazu ein Ansatz. Die Liste mit geeigneten Filmen ist sicher lang – Tabelle 4-8 zeigt eine kleine Auswahl.

Ob Clive Owen als Romeo-Agent, die verlorenen Gerichtsakten von Ben Affleck oder die im Fitness-Studio vergessene CD aus *Burn After Reading* – von all diesen Filmen eignen sich nicht nur ausgewählte Szenen, um Sicherheitsexperten aus der uncoolen Spießer-Ecke herauszuziehen. Zumindest in Filmen sind Sicherheitsexperten intelligent und gutaussehend, sie jetten um die Welt und sind den anderen immer einen Schritt voraus. Ein Image, das nicht schaden kann.

Die genannten Filme sollten in keiner Video-Sammlung von Security-Experten fehlen. Ebenso, wie in deren Bücherregalen Bruce Schneier<sup>96</sup> und Kevin Mitnick<sup>97</sup> nicht fehlen dürfen. Neben der Überzeugungskraft von Filmen verblasst jedes Fachbuch – vor allem bei den Mitarbeitern. Starten Sie doch die nächste Security-Schulung mit einem der Filme aus Tabelle 4-8 oder zeigen Sie zumindest einen Ausschnitt. Sie wären wahrscheinlich der oder die Erste in der Firma, die auf diese Art Schulungen beginnt, und manch einer würde sich an die beliebtesten Schulstunden mit Filmvorführung zurückerinnern. Aber positive Erinnerungen sind gut – besonders wenn sie bei einer Security-Schulung aufkommen. Zeigen Sie z.B. einige Filmausschnitte und lassen Sie Ihre Zuhörer die Filmtitel erraten. Wer die Antwort weiß bekommt ein kleines Give-Away – am besten natürlich mit Security-Bezug. Ihrer Phantasie sind keine Grenzen gesetzt. Zugegeben, diese methodischen Ansätze muten vielleicht etwas experimentell an und sind auch nicht für jede Gruppe geeignet. Jedenfalls sind sie besser geeignet, wie ein belehrender Frontalvortrag, bei dem die Zuhörer sich nach drei Tagen an nichts anderes mehr erinnern, als dass er furchtbar war.

Und nicht nur Filme unterstreichen die Botschaft „*Security ist cool*“. Nehmen wir zum Beispiel die beiden weltweit wichtigsten IT-Security-Konferenzen *blackhat*<sup>98</sup> und *Def Con*<sup>99</sup>: Diese finden jedes Jahr in Las Vegas statt – Spießern wäre sicher ein anderer Ort eingefallen. Überhaupt sehen manche Security-Konferenzen auf den ersten Blick eher wie ein riesen Spaß aus. Die belgische Hacker-Konferenz

---

<sup>96</sup> U.a. Autor des Klassikers *Angewandte Kryptographie*; 2005; Pearson Studium; ISBN: 978-3827372284

<sup>97</sup> U.a. Autor des Buchs *Die Kunst des Einbruchs*; 2008; mitp; ISBN: 978-3826617461

<sup>98</sup> <http://blackhat.com>

<sup>99</sup> <http://defcon.org>

BruCON<sup>100</sup> startet unter dem Motto „*Hacking for Beer*“ – und das bei Partnern, wie Ernst&Young, Cisco oder der ISACA, die man durchaus als seriös bezeichnen kann. Allein diese drei Konferenzen zeichnen ein ganz anderes Bild von IT-Sicherheitsbeauftragten, Datenschützern und Co. als es ihnen im Allgemeinen zugeschrieben wird. Eine Facette, die in jedem Fall ein Blick wert ist, besonders wenn man vor der Aufgabe steht, auch alle Facetten von Persönlichkeiten im Unternehmen oder der Behörde anzusprechen, um sie für Security zu begeistern. Dass diese Aufgabe nur zu lösen ist, wenn man ihnen das Thema ebenso facettenreich aufbereitet, wie sie es aufnehmen, ist man auf dem richtigen Weg, den Erfolg einer Nachricht an der subjektiven Wirkung beim Empfänger zu messen. Man kann es gar nicht oft genug wiederholen: Die Zwänge, Ziele, Prioritäten und Risiken des Empfängers entscheiden darüber, ob eine Nachricht richtig vorgebracht wurde.

Ob man die Botschaft „*Security ist Cool*“ als lohnenswert erachtet oder nicht, hängt also nicht davon ab, ob man sie als Sicherheitsprofi gut findet oder nicht. Denn eines steht fest: Überlässt man diese Botschaft Crackern, Skript-Kidies und Trickbetrügern, dann ist das ein vermeidbares Sicherheitsrisiko. Angreifer werden so von Mitarbeitern sogar als faszinierende Freibeuter gesehen, die eher anziehen als abstoßen<sup>101</sup>.

## 4.6 Tue Gutes und rede darüber

In einem Punkt arbeiten Security-Experten tatsächlich wie die Vorbilder im Film. Sie arbeiten im Verborgenen. Einziger Unterschied: Die Filmhelden gehen mit ihren Erfolgen in gewisser Weise „*an die Öffentlichkeit*“. Kein Wunder, dass sie als heldenhafte Retter der Welt in die Filmgeschichte eingehen und für IT-Sicherheitsbeauftragte, Datenschützer und Co. nur die Reste bleiben. „*Tue Gutes und rede darüber*“, lautet eine Redewendung, die sich Sicherheitsprofis durchaus hinter die Ohren schreiben sollten.

Nur wie macht man das, ohne dabei zum Marktschreier zu verkommen? Diese Frage ist nicht leicht zu beantworten. Manchem liegt es einfach nicht, von den eigenen Erfolgen zu berichten. Wenn man aber nicht ab und an von den eigenen Erfolgen berichtet, ist klar, dass sich bald jemand Gedanken darüber macht, wozu man eigentlich da ist. Erinnern Sie sich an die Szene, mit der auf Seite 7 die Security-Bühne vorgestellt wurde. Als plötzlich das Licht ausgefallen war, sagte der uneinsichtige Schauspieler, dem der Regisseur eben noch zum zehnten Mal

---

<sup>100</sup> <http://brucon.org>

<sup>101</sup> known\_sense (Herausgeber u.a.); Entsicherung am Arbeitsplatz: Die geheime Logik der IT-Security in Unternehmen; 2006; known\_sense; Seite 17

den Text vorgesagt hatte: „Wofür bekommen sie hier eigentlich ihr Geld, wenn da dauernd das Licht ausgeht.“ So bitter es ist: Das kommt dabei heraus, wenn man sich auf Bescheidenheit beschränkt.



**Abbildung 4-9:** Helfen Sie Ihrem Publikum auf die Sprünge

Es ist die Aufgabe der Security-Profis für sich und alle, denen Sicherheit am Herzen liegt, die Werbetrommel zu rühren. Das bedeutet, die internen wie externen Beteiligten dahingehend zu beeinflussen, dass sie dem Thema Sicherheit aufgeschlossener gegenüberstehen.

Gutes Marketing für das Thema Security...

- ❖ ...erhöht die Identifikation aller Beteiligten mit den gesetzten Zielen.
- ❖ ...verbessert die Unterstützung durch die Chefs.
- ❖ ...steigert die Transparenz.
- ❖ ...verbessert das Arbeitsklima im Security-Team und zu den Beteiligten.<sup>102</sup>

Dieser Ansatz geht über das reine Generieren von guten Nachrichten hinaus, wie wir es im Abschnitt Good-Cop – Bad Cop bereits kennengelernt haben. In diesem Abschnitt ging es darum – im Sinne von Neuigkeiten – von der Sache selbst zu berichten während es nun darum geht, die passenden Hintergründe zu liefern und auch nach innen zu werben – also ins Security-Team hinein. Die

---

<sup>102</sup> Johannes Voss; Von Wölfen lernen- effektiv und souverän im Projekt; 2007; Hanser Verlag; ISBN: 9783446409798; Seite 196 ff 

Schlüsselfunktionen müssen dazu in gewisser Weise von der eigenen Leistungsfähigkeit überzeugt werden. Nur wenn dies erreicht wird, kann man auch Außenstehende überzeugen. Ging es im Abschnitt Good-Cop – Bad Cop noch darum nüchterne Nachrichten zu erzeugen, sind jetzt die Waffen des Leitartikels gefragt: Beziehen Sie Stellung zu den Leistungen des Security-Teams. Informationen, die auf jeden Fall weiter gegeben werden sollten, sind:

- ❖ Sinn und Zweck der Sicherheit für die einzelnen Zielgruppen (Nur der Hinweis, dass man Sicherheit macht, um sicher zu sein, reicht natürlich nicht aus.)
- ❖ Hintergründe zu getroffenen Entscheidungen (Zum Beispiel, welches Ziel mit der ISO-Zertifizierung verfolgt wird.)
- ❖ Hintergründe zu den Personen, die dem Security-Team angehören
- ❖ Bereits erreichte Meilensteine
- ❖ Zukünftige Meilensteine

Arbeiten Sie im Gespräch mit Mitarbeitern und Chefs heraus, welche Stärken im Security-Team stecken und hauen Sie sich nicht gegenseitig in die Pfanne. „*Tue Gutes und rede darüber...*“ Die Überschrift dieses Abschnitts könnte man auch so erweitern: „*...und behalte den Rest für Dich.*“

IT-Sicherheitsbeauftragte, Datenschützer und Co. schlecht zu machen, übernehmen schon die Mitarbeiter und Chefs. Man muss den Kritikern dabei nicht noch zur Hand gehen und zum Besten geben, wie schlecht das Datenschutzkonzept, oder wie untauglich die Firewall ist. Keine Frage, solche Mängel müssen angesprochen werden, wenn sie denn bestehen. Sie sind aber sicher keine geeigneten Marketing-Botschaften.

## 4.7 Zusammenfassung

Wir haben in diesem Kapitel einige ergänzende Möglichkeiten kennengelernt, mit denen Security-Maßnahmen mehr Geltung verschafft werden kann. Auch im vierten Kapitel war entscheidend, welche Zielgruppe dabei angesprochen werden sollte. Unternehmen und Behörden in denen eine gewachsene Sicherheitskultur herrscht, unterscheiden sich von solchen, in denen Sicherheitsmaßnahmen strukturiert geplant werden.

Wir haben gesehen, wie ein gutes Zusammenspiel aus guten und schlechten Nachrichten funktionieren kann. Für die meisten Sicherheitsexperten sind nicht die schlechten Nachrichten das Problem: Die Frage lautet eher, woher man gute Nachrichten nehmen soll. Es lohnt sich jedoch, nach ihnen zu suchen. Wie in vielen Bereichen des Lebens lassen sich positive Nachrichten zur Bestärkung aller

Beteiligten einsetzen und verleihen den negativen Nachrichten mehr Gehör. Wer ewig nur von bevorstehenden Katastrophen redet, verliert irgendwann die Zuhörer.

Im Abschnitt über das Security-Storyboard haben wir gesehen, dass die Arbeit von Sicherheitsprofis in gewissen Zyklen verläuft, die wie die Szenen eines Theaterstücks aneinander gereiht sind. In der Realität ist man der Szenenfolge allerdings nicht hilflos ausgeliefert; man kann sie gezielt beeinflussen und so erreichen, möglichst schnell in die vierte Szene zu kommen, in der die Sicherheitsexperten ihren großen Auftritt haben und sich an die Umsetzung ihrer Maßnahmen machen können.

Danach ging es um Avatare – grafische Stellvertreter, die der nächsten Security-Awareness-Kampagne ein Gesicht geben können. Wenn man grobe Fehler vermeidet und bei Planung und Umsetzung die Grundlagen aus den vorangegangenen Kapiteln berücksichtigt, dann können Avatare helfen, die Reichweite und Akzeptanz von Kampagnen zu erhöhen.

Anhand einiger Beispiele wurde gezeigt, dass Security-Experten alles andere als spießig sind. Im Gegenteil: *„Security ist cool.“* Diese Botschaft ist jedoch nicht nur als polarisierende Selbsteinschätzung aufzufassen. Sie ist notwendig, um Cracker, Skript-Kidies und Trickbetrüger aus dieser Ecke zu drängen, in die sie zu Unrecht gerückt werden. Es ist nun mal nicht cool Leute über den Tisch zu ziehen, denn am Ende gewinnt sowieso – na klar – Bruce Willis.

Im letzten Abschnitt ging es schließlich darum, wie wichtig es ist, nicht nur sein Handwerk zu verstehen, sondern es allen Beteiligten mitzuteilen. Wer immer nur im Verborgenen arbeitet, läuft Gefahr als überflüssig wahrgenommen zu werden. Daher lautet die abschließende Botschaft dieses Kapitels: *„Tue Gutes und rede darüber.“*

## 5 Krisenbewältigung

*„Es kann nächste Woche keine Krise geben,  
ich habe keine Termine mehr frei.“*

*Henry Kissinger*

Die bisherigen Kapitel dieses Buchs bauten mit den vorgestellten Ideen und Konzepten in die Zukunft. Der Schwerpunkt galt der Prävention von Security-Konflikten. Nun stellt sich die Frage: *„Was tun, wenn die Security-Krise bereits in vollem Gange ist?“* Wie findet man dann den Weg zurück auf ein Niveau, das ein normales Arbeiten ermöglicht.

Dabei bietet der Alltag den Sicherheitsprofis eine ganze Reihe von Krisen, auf die sie adäquat reagieren müssen. Nicht zuletzt kann auch einem Sicherheitsprofi mal der Kragen platzen. Wie sollte man seinem Ärger dann Luft machen, ohne das Ganze am nächsten Tag zu bereuen? Und wie kommt man stattdessen in dem strittigen Punkt weiter, ohne den Gesprächspartner zu verletzen und damit noch mehr Widerstand zu provozieren? Wenn alles nichts hilft, braucht man ein krisenfestes Instrumentarium, mit dem man auf den persönlichen Angriff reagieren kann: Dazu gehört eine klare Idee, wie man im Unternehmen oder der Behörde auf eskalierende Konflikte reagieren will. Ohne Sie entstehen sonst ärgerliche Nebenkriegsschauplätze, weil man sich zusätzlich der Unterstützung von höherer Stelle rückversichern muss, wenn der Konflikt schon in vollem Gange ist.

Darüberhinaus muss man genau wissen, welche Krisen-Anteile mit Diskretion zu behandeln sind, und welche man gezielt nach draußen geben will. Die Balance zwischen Diskretion und Krisen-PR ist nicht leicht zu finden. Vor allem dann nicht, wenn man sich über diesen Aspekt erst Gedanken macht, wenn man schon mitten im Geschehen steckt.

Die größte Krise ist aber wahrscheinlich die, wenn man von höchster Stelle torpediert wird und die Geschäfts- oder Behördenleitung die Unterstützung versagt. Auch diesem Problem wird sich das folgende Kapitel widmen. In diesem schwierigen Fall – das soll nicht verschwiegen werden – ist für den Erfolg ein starkes Stück Arbeit nötig.

## 5.1 Der Umgang mit Widerstand

Wir haben bereits gesehen, dass es sich lohnt, seinen Gesprächspartnern wertschätzend und durch das Einräumen von Entscheidungsfreiheit gegenüber zu treten. Dies lohnt sich, weil es die Tendenz zum Widerstand reduziert, der durch Bevormundung und Geringschätzung entsteht. Besonders ärgerlich an diesen Widerständen ist, dass sie bei der Verwirklichung der betreffenden Sicherheitsvorhaben im Weg stehen. Der Widerstand wird dabei nicht etwa offen vorgebracht. Gerade wenn es sich um persönliche Motive oder Ängste handelt, wird der Protest in vermeintlich sachliche Argumente verpackt, die unter Umständen zu nicht enden wollenden Streitgesprächen führen können. Selbst, wenn sich die Argumente entkräften lassen, schwelt der Konflikt weiter und lodert in der nächsten Besprechung oder bei anderer Gelegenheit wieder auf. Statt sich endlos wiederkehrenden Konflikten hinzugeben, sollte man den Widerstand aufgreifen, ihm Raum geben und die darin enthaltene Energie in Veränderung umsetzen.<sup>103</sup>

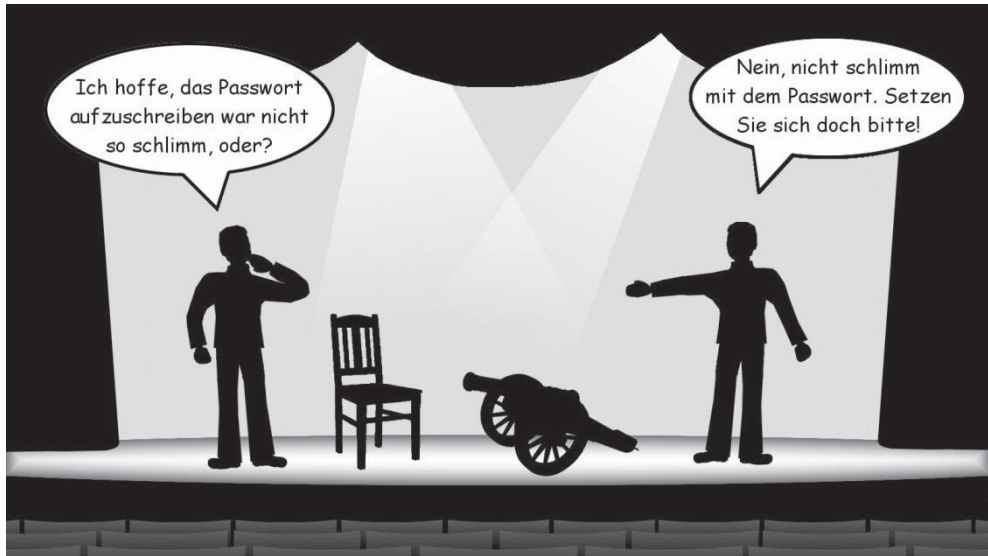
Wie so oft gilt auch bei widerkehrenden Widerständen: „*Ruhe bewahren!*“ Die so entstandene Denkpause sollte genutzt werden, um dem Protest Gehör zu schenken und so den Druck aus der Situation zu nehmen. Sie haben vielleicht schon an sich selbst bemerkt, dass es manchmal ausreicht, Dinge einfach mal ungehindert und ohne Gegenangriff aussprechen zu dürfen, die einem auf der Seele liegen – danach ist alles wieder gut und man kann zurück an die Arbeit. Das gilt auch für Mitarbeiter und Chefs, die mit unliebsamen Sicherheitsmaßnahmen konfrontiert sind: In den allermeisten Fällen wird ihnen dadurch subjektiv die Arbeit erschwert. Auch wenn Sie als Sicherheitsexperte wissen, dass dieses subjektive Empfinden Unschärfen enthält. Für die Betroffenen sind diese Momente der Kritik eine oft sehr emotionale Angelegenheit – eine sachliche Ebene ist zunächst kaum in Sicht. Lassen Sie die Personen sprechen und hören Sie deren Bedenken aufmerksam zu und erkennen Sie deren Bedürfnisse. Nur so können Sie die Ursachen für den Widerstand erforschen und den Einstieg in ein sachliches Gespräch finden, das sich an einer gemeinsamen Problemlösung orientiert.

Auch eine Art von Widerstand: Als verständiger Security-Profi redet und redet man; man schenkt den Problemen von Mitarbeitern und Chefs wieder und wieder Gehör und dann – als hätte man vor Wände gesprochen – passiert ein Sicherheitsvorfall, der natürlich vermeidbar gewesen wäre, wenn sich nur alle an die Vorgaben gehalten hätten. Die Schuldigen zeigen auf das Sicherheits-Team und fragen, warum man sie nicht vor diesem Fehler bewahrt habe. Nun sind es nicht

---

<sup>103</sup> Carola Bohren Meyer, Rita-Maria Züger; Konfliktbewältigung im Team - Leadership-Basiskompetenz; 2007; Compendio Bildungsmedien AG; ISBN: 9783715593364; Seite 70  
R

die Mitarbeiter, bei denen die Emotionen hochkochen, sondern die IT-Sicherheitsbeauftragten, Datenschützer und Co. Wie bringt man seine Emotionen dann am geschicktesten vor? Sie einfach hinunter zu schlucken ist ebenso wenig angebracht, wie sich in einem Wutanfall zu verlieren.



**Abbildung 5-1:** Nicht gleich mit Kanonen auf „Spatzen“ schießen

Den Ärger in sich hinein zu fressen, oder das Problem einfach zu verdrängen ist jedoch sicher auch keine gute Lösung. Wenn man sich über etwas ärgert, dann ist es durchaus erlaubt, diesen Ärger auch mitzuteilen. Ebenso wie es für Mitarbeiter erlaubt ist ihre Kritik vorzubringen, ist das natürlich auch für Security-Experten erlaubt. Einzige Bedingung: Der Ärger muss in geregelte Bahnen geleitet werden. Das Fünf-Schritte-Modell<sup>104</sup> hilft weiter, die Emotion in geregelten Bahnen auszudrücken. Es ermöglicht, auch in emotionalen Situationen am Thema zu bleiben und ein sachliches Gespräch über diese Emotion zu beginnen, ohne dabei den Gesprächspartner anzugreifen oder zu beleidigen. Wenn man negative Emotionen vorbringen möchte, dann sollten diese ihrerseits nicht neue Emotionen auslösen. Die Gefahr einer Eskalation wäre viel zu groß.

Man sollte dabei nicht vergessen, dass einem emotionalen Mitarbeiter in den meisten Fällen von den anderen Mitarbeitern Verständnis entgegengebracht wird, weil sie seine Motive nachvollziehen können. Der Nörgler kann sich dadurch ein

<sup>104</sup> Susanne Klein; Wenn die anderen das Problem sind: Konfliktmanagement, Konfliktcoaching, Konfliktmediation; 2006, GABAL-Verlag GmbH; ISBN: 3897495864; Seite 146

Stück weit in der Masse verstecken. Wenn jedoch dem IT-Sicherheitsbeauftragten oder dem Datenschutzler auf dem Flur der Kragen platzt, dann redet davon die gesamte Belegschaft und alle haben Verständnis für den, der sich den Anpfiff eingefangen hat. Im Sinne der Sicherheit ist es natürlich kontraproduktiv, wenn sich die Mitarbeiter mit dem solidarisieren, der gegen Sicherheitsbestimmungen verstoßen hat.

| Die fünf Schritte | Inhalt                                               |
|-------------------|------------------------------------------------------|
| 1. Schritt        | Wer hat die Emotion?                                 |
| 2. Schritt        | Was ist es für eine Emotion?                         |
| 3. Schritt        | Wie wurde die Emotion ausgelöst?                     |
| 4. Schritt        | Warum ist die Emotion gerade in diesem Fall so groß? |
| 5. Schritt        | Welche subjektive Interpretation resultiert daraus?  |

**Tabelle 5-1:** Emotionen kanalisieren: Das Fünf-Schritte-Modell

Das wichtigste ist zunächst Ruhe zu bewahren und sich genau zu überlegen, wie man den Ärger zu Wort bringen will. In Tabelle 5-1 sind die fünf wichtigsten Botschaften aus dem Fünf-Schritte-Modell enthalten, die ein sachliches Gespräch über den entstandenen Ärger ermöglichen. Betrachten wir das folgende Beispiel.

### 5.1.1 Fallbeispiel: Bob platzt der Kragen

Malory arbeitet im Vertrieb der ExAmple AG und verschickt regelmäßig per E-Mail diverse Spaß-Programme und unglaublich lustige Power-Point Präsentationen an die halbe Firma. Das Risiko, dass auf diese Art und Weise Schadsoftware in die Firma gelangt, ist nicht unerheblich. Der IT-Sicherheitsbeauftragte Bob hatte das Thema bereits mehrfach mit ihm besprochen. Als er nun ohne weiter nachzudenken einen kleinen, auf der Taskleiste des PCs tanzenden Weihnachtsmann an seinen Spaß-Verteiler weiterleitet, den er von einem Kunden aus China zugeschickt bekommen hat, ist Bob außer sich vor Wut.

Am liebsten würde er Malory für drei Wochen im Keller einsperren. Ihm geht es nicht mehr nur um das Sicherheitsproblem, sondern um den wiederholten Ärger, den er mit dem Mitarbeiter hat. Er versucht sich abzuregen und bittet Alice, die Datenschutzbeauftragte, für morgen einen Termin mit Malory auszumachen. Das verhindert, dass er ihn gleich am Telefon anfährt.

Wie muss Bob das morgige Gespräch beginnen? Im 1. Schritt geht es um die Beantwortung der Frage, wer die Emotion hat. Da Bob für sich selbst spricht, muss er mit der ersten Person Singular beginnen. Der Anfang scheint nicht besonders schwer, vermeidet aber die gefährlichen Du-Botschaften<sup>105</sup>, die Gespräche leicht aus dem Ruder laufen lassen. Es geht um Bobs Emotionen und nicht darum, Malory zu sagen, was er für einer ist. Bob beginnt also wie folgt:

*„Ich bin...“*

Im 2.Schritt muss Bob ein Wort hinzufügen, das die Emotion beschreibt, die er empfindet:

*„...sehr verärgert,...“*

Natürlich muss Bob nicht die ganze Zeit nur von sich sprechen, nur um Du-Botschaften zu vermeiden. Bob könnte zwar sagen *„...über Sie!“*, es gibt aber eine bessere Lösung: Er muss von der Sache sprechen. Im 3. Schritt geht es also um das Ereignis, dass die Emotion ausgelöst hat:

*„...dass Sie zum wiederholten Mal E-Mails mit Spaß-Programmen an alle Mitarbeiter geschickt haben,...“*

Malory könnte jetzt dazwischen fahren und sagen: *„Alle anderen haben sich gefreut – soll ich Sie in den Verteiler aufnehmen?“* Um das zu vermeiden muss Bob im 4. Schritt die Begründung nennen, warum die Emotion so stark ist:

*„...obwohl das in unseren Richtlinien verboten ist und ich Ihnen schon mehrfach die Bedeutung dieser Maßnahme erklärt habe...“*

Bis hier her OK. Aber warum so ärgerlich? Im 5. Schritt muss Bob beschreiben, wie er das Verhalten von Malory interpretiert:

*„...und das habe ich so interpretiert, dass Sie weder die Gefahr, die damit verbunden ist, noch meine Fachexpertise ernst nehmen.“*

Damit ist alles gesagt, um ein sachliches Gespräch über diese emotionale Situation zu beginnen. Bob muss nun auf dieser Schiene weiter fahren und kann dabei auch

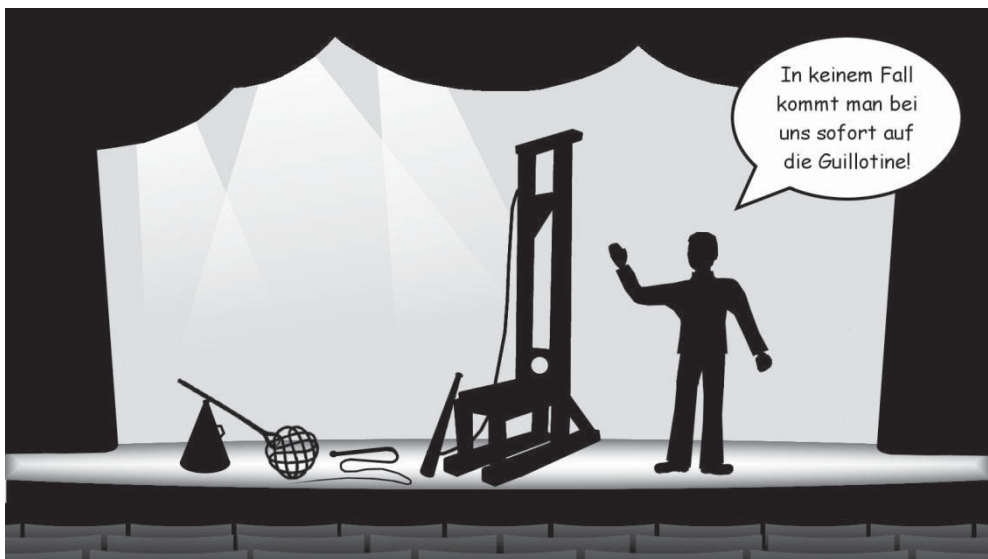
---

<sup>105</sup> Peter R. Wellhöfer; Schlüsselqualifikation Sozialkompetenz: Theorie und Trainingsbeispiele; 2004; UTB; ISBN: 9783825225162; Seite 157 

zum Beispiel auf die Konfliktpipeline zurückgreifen, um das Gespräch zu einer gemeinsamen Lösung zu führen (siehe Seite 82).

## 5.2 Eskalationsstufen generieren

Wer mit Emotionen übers Ziel hinaus schießt, erlebt die gleiche Gegenwehr, wie jemand, der immer mit den sprichwörtlichen Kanonen auf Spatzen schießt. Selbst, wenn er das – im Sinne der konfliktpräventiven Kommunikation - klar, treffend, knapp und wertfrei tut. Wer Mitarbeiter, Teamleitungen und Chefs in Security-Fragen betreut, braucht transparente Eskalationsstufen. Was kann man den Leuten einfach „durchgehen lassen“ und wo muss man entschieden einschreiten? Wie stimmt man die Eskalationsstufen mit den Teamleitungen und Chefs ab? Zum Beispiel landet der Datenschutzbeauftragte im Abseits, wenn er sich schon auf Eskalationsstufe drei befindet, wenn der Chef regelmäßig noch auf Stufe eins steht und alles relativiert.



**Abbildung 5-2:** Die härtesten Sanktionen sind nur als Drohkulisse sinnvoll

Bevor wir uns jedoch mit der gezielten und gewollten Eskalation auseinandersetzen, müssen wir einen Blick darauf werfen, in welchen Stufen Konflikte unkontrolliert eskalieren. Erst, wenn man weiß, auf welcher Stufe der Eskalationsleiter man sich befindet, kann man gezielte Gegenfeuer legen. Man kann drei Phasen der unkontrollierten Konflikteskalation unterscheiden. In jeder

der Phasen lassen sich drei Eskalationsstufen einordnen, entlang derer sich der Konflikt vom Gesunden ins unsinnig Verlustreiche wandeln kann<sup>106</sup>:

❖ **Win-Win**

Konflikte in dieser Phase verlaufen noch für beide Parteien befriedigend, so dass jeder seine Ziele in einer gemeinsamen Lösung erreichen kann. Externe Hilfe ist dazu nicht nötig. Das ist die Art von Konflikten, wie wir sie im Abschnitt 3.3 zur Konfliktpipeline kennen gelernt haben.

❖ **Win-Lose**

In dieser Phase verlieren die Beteiligten den Glauben daran, dass beide ihre Ziele verwirklichen können. Beide Parteien versuchen nur noch die eigenen Ziele durchzusetzen. Spätestens in dieser zweiten Phase ist Hilfe von außen nötig.

❖ **Lose-Lose**

Die Beteiligten haben sich damit abgefunden, dass beide ihre Ziele abschreiben können. Es geht nur noch darum, den Schaden beim jeweiligen Gegenüber zu maximieren und den eigenen zu begrenzen. Ohne Hilfe von außen gibt es für die Streithähne keinen Ausweg.

| Konflikt-Phase   | Eskalationsstufe                      |
|------------------|---------------------------------------|
| <b>Win-Win</b>   | Verhärtung                            |
|                  | Debatte                               |
|                  | Taten statt Worte                     |
| <b>Win-Lose</b>  | Koalition                             |
|                  | Demaskierungen                        |
|                  | Drohstrategien                        |
| <b>Lose-Lose</b> | Begrenzte Vernichtungsschläge         |
|                  | Zersplitterung der Existenzgrundlagen |
|                  | Gemeinsam in den Abgrund              |

**Tabelle 5-2:** Konflikt-Phasen und Eskalationsstufen

<sup>106</sup> Susanne Klein; Wenn die anderen das Problem sind: Konfliktmanagement, Konfliktcoaching, Konfliktmediation; 2006, GABAL-Verlag GmbH; ISBN: 3897495864; Seite 47 ff 

Entlang dieser drei Phasen stehen die neun Eskalationsstufen von Konflikten. Die Grenzen zwischen den Stufen werden von den Beteiligten als gewisse Hemmschwelle wahrgenommen, in die nächste Stufe einzutreten. Werden von keiner Seite gezielte Maßnahmen der Deeskalation ergriffen, ist der Schritt auf die nächste Stufe unausweichlich.

**Phase 1:** Auf der Stufe der *Verhärtung* gibt es eigentlich noch gar keinen richtigen Konflikt. Die Gesprächspartner können einfach die Meinung des Anderen nicht nachvollziehen und zweifeln zunehmend, ob das Gegenüber wirklich ernsthaft an einer Lösung interessiert ist. Auf der Stufe der *Debatte* bestimmen Konkurrenz und Überheblichkeit die Situation und es beginnt eine Schwarz-weiß-Sicht auf das Thema. Man ist überzeugt, dass der Andere nur nach dem eigenen Vorteil handelt. Auf der nächsten Stufe folgen *Taten statt Worte*, weil alles Reden offensichtlich nichts bringt. Ein Projektionsmechanismus setzt ein und man erwartet vom Gegenüber genau das, was man selbst nicht bereit ist preiszugeben. Die Schuld an der ganzen Misere wird der anderen Seite zugeschoben.

**Phase 2:** Die Konfliktparteien werden zunehmend feindselig und suchen nach *Koalitionen*. Die Abwertung der Gegenseite dient gleichzeitig der eigenen Aufwertung. Außenstehende werden in den Konflikt mit einbezogen. Für beide Parteien ergeben sich dadurch Abhängigkeiten von den Verbündeten. Auf der Stufe der *Demaskierungen* geht es darum, das eigene Feindbild auszubauen. Dem Gegenüber werden von Anfang an schlechte Absichten unterstellt und der Konflikt geht mehr und mehr um Werte. Das gegenseitige Vertrauen ist verloren und beide Parteien sind sich sicher, dass der Konflikt nicht mehr zu lösen ist. Auf der Stufe der *Drohstrategien* werden gezielt Drohungen ausgesprochen und Vergeltungsmaßnahmen in Aussicht gestellt, um den Konkurrenten einzuschüchtern. Noch existiert ein Mindestmaß an Kommunikation.

**Phase 3:** In der dritten Phase ist bei jedem die Überzeugung verloren gegangen, dass man seine Ziele noch erreichen kann. Wenn sich die Möglichkeit dazu ergibt, werden *begrenzte Vernichtungsschläge* gegen die andere Partei geführt, auch wenn dies nichts mehr mit den eigenen Zielen zu tun hat. Es geht darum den Schaden des Anderen zu maximieren. Auf

der nächsten Stufe sind die Parteien so weit zerrüttet, dass sie sogar eine *Zersplitterung der Existenzgrundlagen* in Kauf nehmen. Letzte ethische Hemmschwellen werden auf dieser Stufe fallen gelassen. Auf der letzten Stufe fällt sogar die Scheu vor Maßnahmen, die einen eigenen Schaden beinhalten: Besser *gemeinsam in den Abgrund*, als dem Gegenüber einen Vorteil zu gönnen.

| Eskalationsstufe                      | Beispiel                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verhärtung                            | Eine Sicherheitsmaßnahme kommt nicht gut an. Ein Mitarbeiter äußert Unverständnis.                                                                                                                                                                                                                                                                                                            |
| Debatte                               | Die Sicherheitsmaßnahme wird weiter in Frage gestellt: <i>„Der Sicherheitsbeauftragte will sich doch nur profilieren – Sinn ergibt das alles nicht.“</i>                                                                                                                                                                                                                                      |
| Taten statt Worte                     | Die Sicherheitsmaßnahme wird ignoriert, da ja offensichtlich keinerlei Gesprächsbereitschaft besteht.                                                                                                                                                                                                                                                                                         |
| Koalition                             | Der Mitarbeiter sucht Verbündete, denen er erzählt, dass man die Sicherheitsmaßnahme missachten kann, ohne dass der Sicherheitsbeauftragte eingreift.                                                                                                                                                                                                                                         |
| Demaskierungen                        | Der Mitarbeiter unterstellt dem Sicherheitsbeauftragten böse Absichten und stachelt andere auf, ebenfalls nach Schwächen im System zu suchen.                                                                                                                                                                                                                                                 |
| Drohstrategien                        | Der Mitarbeiter droht damit, auch wichtige Sicherheitsmaßnahmen umgehen zu können.                                                                                                                                                                                                                                                                                                            |
| Begrenzte Vernichtungsschläge         | Kann ein Vorfall <i>„proviziert“</i> werden, so wird diese Situation ausgenutzt: <i>„Ach, die unterbrechungsfreie Stromversorgung der Server ist defekt? Zum Wechseln der Birnen an der Zimmerbeleuchtung sollte man doch die Sicherungen raus machen, oder? Au weia, da hab ich wohl die Sicherung vom Serverraum erwischt. Komisch, dass die Server vor so etwas nicht geschützt sind.“</i> |
| Zersplitterung der Existenzgrundlagen | Das bei einem Administrator gefundene Admin-Passwort für den Webserver wird in einem Hacker-Forum veröffentlicht.                                                                                                                                                                                                                                                                             |
| Gemeinsam in den Abgrund              | Informationsdiebstahl, Angriffe, Spionage. Auf dieser Stufe gibt es keine Hemmungen mehr.                                                                                                                                                                                                                                                                                                     |

**Tabelle 5-3:** Beispiele von Security-Konflikten

Diese Eskalationsstufen sind alle auf der Security-Bühne anzutreffen und müssen entsprechend behandelt werden, um den Schritt auf die nächste Stufe zu verhindern. Dazu sollte man für alle Konflikte, die sich in Phase 2 befinden ein aktives Konflikt-Monitoring betreiben. In Tabelle 5-3 wird ein Beispiel Schritt für Schritt durchgespielt.

Die dritte Eskalationsstufe ist die erste, die ein Sicherheitsrisiko darstellt, dass mit jeder Stufe weiter wächst. Diese Eskalationsstufen müssen mit der Geschäfts- oder Behördenleitung besprochen werden. Ziel dieser Absprache ist es, ein gemeinsames Verständnis zu Maßnahmen für die einzelnen Eskalationsstufen zu erreichen. Das Sicherheitsteam muss sich dieser Maßnahmen rückversichern und sich der Unterstützung des Chefs sicher sein. Diese Art von Konflikten beinhalten erhebliche Risiken für die Firma oder die Behörde. In letzter Konsequenz sind sie sogar existenzbedrohend.

Auf der Stufe *Taten statt Worte* brauchen Sicherheitsprofis erste Unterstützung von Vorgesetzten der Linienorganisation. Dem Mitarbeiter muss klar gemacht werden, dass er dabei ist eine Grenze zu überschreiten, die nicht akzeptiert wird. Man darf dabei aber nicht zu hoch ansetzen und dafür sorgen, dass der nächste unzufriedene Mitarbeiter den Prozess durch die Stufen 3 bis 6 nur im Geiste durchmacht, weil er schlimme Sanktionen befürchtet und dann – auf Stufe 7 angekommen – direkt die Sicherungen für den Serverraum raushaut. Daher müssen die Sanktionen dosiert werden und auch für die letzten Stufen der Konflikt-Leiter muss noch eine Steigerungsmöglichkeit vorhanden sein. Wer gleich zu Beginn mit der Kündigung droht, und diese dann nicht umsetzen kann, der verliert alle Möglichkeiten, steuernd auf die Eskalation des Konflikts einwirken zu können.

### 5.2.1 Fallbeispiel: Die ExAmple AG „eskaliert“

Die Datenschutzbeauftragte Alice, der IT-Sicherheitsbeauftragten Bob und Dave, der Sicherheitsbeauftragte haben sich darauf verständigt, dass sie eine klare Linie brauchen, wie im Unternehmen mit eskalierenden Security-Konflikten umgegangen werden soll. Der Chef ist einverstanden. Er hat im Laufe der letzten Zeit, mit Vorführungen, Pen-Tests und Awareness-Kampagnen eingesehen, dass die drei Unterstützung von ihm brauchen. Er will von seinem Security-Team „*einen Vorschlag, wie mit renitenten Mitarbeitern umgegangen werden soll*“.

Alice, Bob und Dave sind sich einig, dass sie die Probleme in der ersten Phase der Eskalationsstufen selbst meistern können. Wenn sich ein Mitarbeiter gegen eine Maßnahme auflehnt, wollen sie mit ihm oder ihr ein klärendes Gespräch führen, mit dem Ziel ein gemeinsam erarbeitetes Protokoll zu erstellen, in dem das Ergebnis dokumentiert wird. Spätestens jedoch, wenn ein Mitarbeiter versucht,

andere mit ins Boot zu holen und Stimmung gegen das Team zu machen, sollen die Vorgesetzten aus der Linie unterstützen. Ein formelles Gespräch mit dem Störenfried beim direkten Vorgesetzten soll dafür ausreichen. Alice, Bob und Dave wollen damit klar machen, dass zwar noch nicht die ganz große Keule ausgepackt wird. Es soll jedoch ebenso klar sein, dass es so nicht weiter geht. Wenn auch das nicht hilft, soll es in der Linienorganisation einen Schritt weiter nach oben gehen. Wenn ein Mitarbeiter der Forschungsabteilung partout nichts einsehen will, dann soll der Forschungsleiter klare Worte finden und diese schriftlich fixieren. Auf diese Art würde er ein gutes Stück der Verantwortung übernehmen, das Thema aus der Welt zu schaffen. Erst danach sollen arbeitsrechtliche Konsequenzen auf dem Plan stehen. Die drei erstellen dazu die folgende Tabelle:

| Eskalationsstufe                      | Maßnahme                                                            | Ebene                                   |
|---------------------------------------|---------------------------------------------------------------------|-----------------------------------------|
| Verhärtung                            | Informelles Gespräch                                                | Security-Team                           |
| Debatte                               | Formelles Gespräch                                                  | Security-Team                           |
| Taten statt Worte                     | Klärendes Gespräch mit Protokoll <sup>107</sup>                     | Security-Team                           |
| Koalition                             | Formelles Gespräch beim direkten Vorgesetzten                       | Security-Team und direkter Vorgesetzter |
| Demaskierungen                        | Klärendes Gespräch mit Protokoll beim Bereichsleiter <sup>108</sup> | Security-Team und Bereichsleiter        |
| Drohstrategien                        | Klärendes Gespräch und Abmahnung                                    | Security-Team und Geschäftsführung      |
| Begrenzte Vernichtungsschläge         | Kündigung                                                           | Geschäftsführung                        |
| Zersplitterung der Existenzgrundlagen |                                                                     |                                         |
| Gemeinsam in den Abgrund              |                                                                     |                                         |

**Tabelle 5-4:** Die Eskalationsstufen der ExAmple AG

<sup>107</sup> Zum Verlauf der Gespräche siehe Abschnitt 3.3 „Konfliktpipeline“

<sup>108</sup> Als Drohkulisse soll ab dieser Stufe im Einzelfall eine Kündigung möglich sein.

Der Chef ist einverstanden, den Vorschlag in der nächsten Runde mit den Bereichsleitern zu besprechen. Alice soll dazu eine Präsentation vorbereiten und die Eskalationsstufen der ExAmple AG vorstellen.

### 5.3 Diskretion bei Sicherheitsvorfällen

Bei Sicherheitsvorfällen ist Diskretion nach außen geboten, um das Unternehmen vor Imageverlusten zu bewahren. Sicherheitsvorfälle sind eben nicht die beste Werbung für ein Unternehmen. Selbst dann nicht, wenn man zu berichten hätte, dass der Sicherheitsvorfall hervorragend abgearbeitet werden konnte. Die Grundlage für eine Diskretion nach außen ist die interne Diskretion: Nicht jeder im Unternehmen muss von einem aktuellen Sicherheitsvorfall erfahren. Aber Vorsicht: Es geht bei Sicherheitsvorfällen um die Reputation des Unternehmens. Das bedeutet, dass es einige wenige Mitarbeiter im Unternehmen gibt, die sofort und umfassend zu informieren sind. Dazu später.

Die interne Diskretion ist aber nicht nur aus Sicht des Unternehmens wichtig. Auch die involvierten Mitarbeiter haben in Krisenzeiten etwas zu verlieren. Stellen Sie sich vor, auf der lokalen Festplatte eines Mitarbeiters werden anzügliche Filme gefunden. Der Verdacht liegt nahe, dass er die Dateien dorthin abgelegt hat. Hier ist besonnenes Vorgehen gefragt. Es kann genauso sein, dass der Administrator, oder der Vorbesitzer des PCs die Dateien dort abgelegt hat. Selbst wenn sich hinterher die Unschuld des Betroffenen nachweisen lässt – seinen guten Ruf ist er erst mal los. Zumindest wird er ihn während der Zeit der Ermittlungen los sein, wenn die Sache nicht mit der nötigen Diskretion behandelt wird.

Die Frage lautet: Wie schottet man Sicherheitsvorfälle vor zu vielen Augen und Ohren ab, ohne genau dadurch aufzufallen. Stellen Sie sich vor, der IT-Sicherheitsbeauftragte Bob und der Forschungsleiter würden plötzlich mit viel Tamtam und mit dem Forensik-Koffer bewaffnet im Büro des Mitarbeiters Jeff erscheinen. Seine zwei Kolleginnen würden sie des Raumes verweisen: *„Das sind zu persönliche Sachen um die es hier geht.“* Erst nach zwei Stunden kämen sie wieder raus und Jeff bleibt angeschlagen zurück. Das würde die Gerüchteküche natürlich ordentlich anheizen. Wie soll man in solchen Fällen aber sonst vorgehen? Man kann je schlecht bis Feierabend warten oder bis zum Wochenende? Oder doch?

In der Tat sollte man sich die Frage nach dem richtigen Zeitpunkt stellen. Die Schadensabwendung vom Unternehmen und die von den Mitarbeitern, müssen gegeneinander abgewogen werden. Handelt es sich tatsächlich *„nur“* um anzügliche Bilder kann man sicher einen besseren Moment abwarten, während bei installierten und funktionsfähigen Hacker-Tools sicher mehr Eile geboten ist.



**Abbildung 5-3:** Ziemlich auffällig: Die Mauer des Schweigens bei Sicherheitsvorfällen

Im ersten Schritt müssen dabei technische Aspekte berücksichtigt werden. Danach – jedoch nicht minder wichtig – müssen im zweiten Schritt die Interessen der Beteiligten gegeneinander abgewogen werden. Im Rahmen der Abarbeitung von Sicherheitsvorfällen können Sicherheitsexperten viel von ihrem mühsam aufgebauten Vertrauen verlieren. Wenn dies zur Abwendung einer akuten Gefahr nötig ist, dann wird man diesen Vertrauensverlust wohl oder übel verkraften müssen. Man sollte jedoch den Schaden nicht unterschätzen, der durch eine gestörte Kommunikation zum Security-Team entsteht. Bei der Entscheidung, ob unmittelbares Handeln erforderlich ist oder nicht, sind eine ganze Reihe Fragen zu klären:

- ❖ Steht ein Angriff unmittelbar bevor, findet er bereits statt, oder ist dies zu befürchten? Beispiele:
  - Durch einen aktiven Trojaner besteht Zugriff auf vertrauliche Unternehmensdaten.
  - Es wurden mehrere Trojaner vom Virenschanner erkannt und in Quarantäne gestellt.
- ❖ Besteht die Gefahr, dass durch den Betroffenen Beweismittel vernichtet werden könnten? Beispiele:
  - Der Betroffene weiß bereits, dass Unregelmäßigkeiten bei ihm aufgefallen sind.
  - Der Betroffene befindet sich zum Zeitpunkt des Vorfalls auf einer Dienstreise.
- ❖ Besteht der konkrete Verdacht einer Straftat? Beispiele:

- Durch die Straftaten wurde Leib und Leben gefährdet.
- Es handelt sich um Straftaten mit rassistischem Hintergrund.
- Es geht es um den Verdacht einer Urheberrechtsverletzung.
- ❖ Kann der Umfang des Vorfalls alleine bewältigt werden? Beispiele:
  - Das Security-Team hat keine forensischen Möglichkeiten.
  - Es ist wahrscheinlich, dass es sich um Industriespionage handelt.
- ❖ ...

Die Liste der Fragen kann beliebig fortgeführt werden. Insbesondere ist sie davon abhängig, in welchem Unternehmen oder welcher Behörde man tätig ist. Stellen Sie sich vor, auf der lokalen Festplatte eines PCs werden Bilder von Totenköpfen gefunden. Das eine Bundeswehr-Dienststelle in so einem Fall anders reagiert, wie eine Spedition ist jedem klar, der sich an den Totenkopf-Skandal erinnert.<sup>109</sup> Auch ist es ein Unterschied, ob ein Vorfall in einer Polizeidienststelle passiert oder in einem anderen Unternehmen. Wenn die Musikindustrie Ihr bester Kunde ist, haben raubkopierte mp3s im Firmennetz eine andere Bedeutung für Ihr Unternehmen, wie wenn Ihre Hauptkunden alle Anhänger der Piratenpartei sind<sup>110</sup>. Das soll nicht heißen, dass es für manche Firmen strafbare Handlungen erster und zweiter Klasse gibt. Eine solche Betrachtung soll den Philosophen und Politikern vorbehalten bleiben. Für Sicherheitsexperten gibt es nur Straftaten mit großen Auswirkungen auf ihre Arbeit und solche, die eher wenig Arbeit machen.

In jedem Fall sollten Sie für Ihr Unternehmen eine Liste mit Fragen erarbeiten, welche Szenarien für Sie eine Betrachtung wert wären. Was wäre denn ihr Super-GAU? In welchen Fällen hätte innere wie äußere Diskretion für Ihr Unternehmen oder Ihre Behörde höchste Priorität? Bei der Bewältigung eines Vorfalls kann nichts Schlimmeres passieren, als sich diese Fragen erst dann stellen zu müssen, wenn das Kind bereits in den Brunnen gefallen ist und man zum Handeln gezwungen ist. Wenn es soweit ist, werden Sie jedenfalls keine Zeit mehr haben, Ihre Entscheidung abzuwägen und diese auf Grundlage einer reiflichen Überlegung zu treffen. Im Gegenteil: Wenn Sie keine Vorkehrungen getroffen haben, die Ihnen die Entscheidung erleichtern, werden Sie aus dem Bauch heraus handeln müssen und mit ziemlicher Wahrscheinlichkeit daneben liegen.

Wenn man jedoch bei Vorfällen Diskretion wahren soll, wie sollen die Mitarbeiter und Chefs dann mitbekommen, dass auch für das eigene Unternehmen eine ganz reale Bedrohung existiert? Übertragen Sie diese Frage auf das Problem eines

---

<sup>109</sup> Die Bundeswehr war 2006 durch Bilder in die Schlagzeilen gekommen, auf denen sich deutsche Soldaten in Afghanistan in zweifelhaften Posen mit Totenschädeln zeigten. Ich war zu diesem Zeitpunkt als IT-Sicherheitsbeauftragter des Afghanistan-Einsatzes in Masar-e Sharif und erinnere mich ganz gut an die ausgedehnte Suche.

<sup>110</sup> <http://wiki.piratenpartei.de/Urheberrecht>

forschenden Mediziners: Handelt dieser indiskret, wenn er seine Forschungsergebnisse veröffentlicht, in denen er schildert, wie es seinen Patienten ergangen ist? Mitnichten. Das ist nur dann der Fall, wenn man aufgrund der Ergebnisse auf einen bestimmten Fall zurückschließen könnte oder gar Namen veröffentlicht würden. In allen anderen Fällen erwartet man von einem Arzt sogar, dass er seine Forschungsergebnisse mit anderen Ärzten und der Öffentlichkeit teilt. Das gleiche muss für Security-Experten gelten.

Während Betrachtungen zur Frage der internen Diskretion weitestgehend autark angestrengt werden können, ist äußere Diskretion immer von innerer Diskretion abhängig. Sobald ein Vorfall intern bekannt ist, müssen Maßnahmen vorbereitet werden, wie man reagieren will, wenn er extern bekannt wird. Darüberhinaus muss ein Personenkreis festgelegt werden, der von der internen Diskretion ausgeschlossen ist. Dies würde beispielsweise den Pressesprecher betreffen, der zumindest informiert werden muss, dass es einen Vorfall gab, und wie er sich verhalten soll, wenn er darauf angesprochen wird – insbesondere, was fachliche Verlautbarungen anbetrifft. Sätze wie *„unser hochqualifiziertes Security-Team hat alles im Griff“*, sind in Pressemitteilungen Tabu. Man fordert den geneigten Leser ja geradezu heraus, diese Qualifikation aufgrund des Vorfalls in Frage zu stellen. Wenn man dann drei Tage später nachschieben muss, dass ein seit Monaten nicht gepatchter Server die Schuld am Ausfall der Webseite trug, kommt man in Erklärungsnöte. Das Thema Krisen-PR wird jedoch erst im nächsten Abschnitt betrachtet. Für den Moment reicht die Erkenntnis, dass einige Personen im Unternehmen oder der Behörde – gerade in den Fällen höchster Diskretion – ein ganz besonderes Informationsinteresse haben.

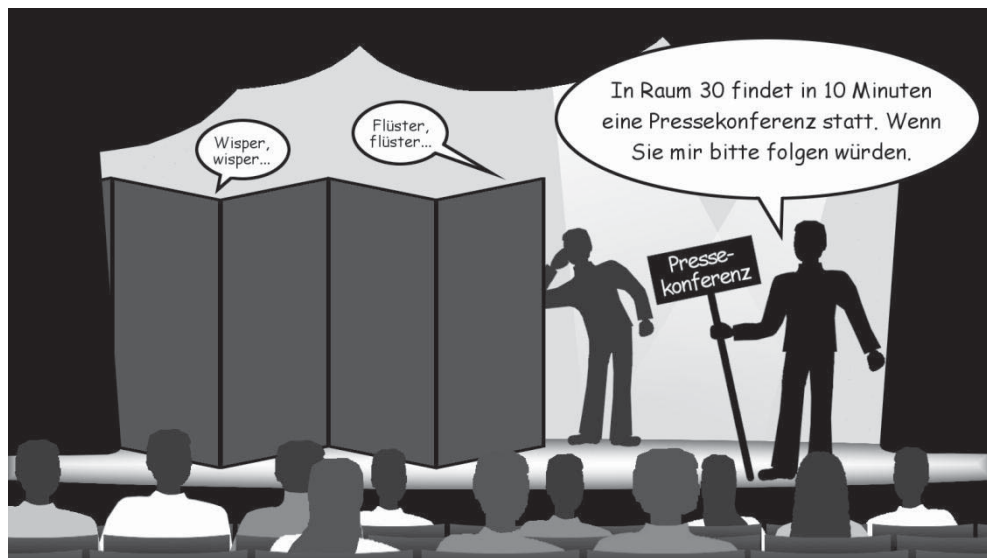
Dieser Personenkreis ist je nach Schadensausmaß unterschiedlich. Ein Beispiel, dass Sie bitte selbst gedanklich durchspielen: Der Server und einige Rechner der Finanzbuchhaltung könnten beschlagnahmt werden, weil dort Bildmaterial gefunden wurde, dessen Besitz strafbar ist. Was meinen Sie, was auf den betroffenen Festplatten noch so alles gefunden werden könnte? Für manchen Chef könnte das der eigentliche Sicherheitsvorfall sein. Wenn Sie eine solche Herausforderung im Alleingang *„vermasseln“*, sitzen Sie sicher bis zum Sankt Nimmerleinstag in der Buhmann-Falle – ohne Aussicht auf Rettung.

Aus diesen Überlegungen ergeben sich zwei Anforderungen an einen diskreten Umgang mit Sicherheitsvorfällen: Erstens müssen Rahmenbedingungen und Szenarien festgelegt werden, die es ermöglichen Vorfälle danach zu bewerten, wie wichtig Diskretion für das Unternehmen oder die Behörde ist. Und zweitens müssen Personen identifiziert werden, die von dieser Diskretion ausgenommen sind und im Falle des Falles ein besonderes Informationsinteresse haben.

## 5.4 Krisen-PR

Im vorigen Abschnitt ging es darum, Diskretion zu wahren und einen Personenkreis zu bestimmen, der trotzdem umfassend zu informieren ist. Eine Aufgabe, die für jedes Unternehmen individuell zu erledigen ist. Nun geht es darum, gezielt die Informationen zu veröffentlichen, die bei der Abarbeitung eines Vorfalls hilfreich sind – intern wie extern. Wer wie in Abbildung 5-3 die Schotten ganz dicht macht, der riskiert Eigeninitiative. Wer neugierig genug ist, fängt gerade wegen der Mauer des Schweigens an zu suchen. Möglicherweise erfährt er so mehr als uns lieb sein kann oder – was noch schlimmer wäre – falsche Informationen, die man dann wenig glaubwürdig dementieren muss.

Der mit einer solchen Informationskampagne verbundene Aufwand ist leicht zu unterschätzen. Welche Stellen sind wie zu informieren und wie kann man sich auf diesen Informationsfluss vorbereiten? Ist der Vorfall da, sind alle Augen auf den Security-Manager gerichtet und der steht unter Druck. Interne Mails voller Schreibfehler sind da nur der Anfang. Die Frage lautet: Wie „verkauft“ man sich in Krisenzeiten und wie kann man vorsorgen. Mit der richtigen Krisen-PR geht man gestärkt aus Vorfällen hervor.



**Abbildung 5-4:** Krisen-PR informiert und lenkt zugleich ab

Eigentlich scheint es gar nicht lohnenswert, sich mit dem Thema Krisen-PR auseinander zu setzen. Sollte man doch davon ausgehen, dass Krisen-PR ein selbstverständlicher Bestandteil allgemeiner PR ist. Public Relations in der Krise bedient sich also auch nicht grundsätzlich anderer Mittel und Tools zur internen

und externen Kommunikation. Nur der thematische Schwerpunkt ist in Krisenzeiten anders gelagert. Er konzentriert sich auf die folgenden drei Aspekte:

- ❖ Aktives vorbeugen von Krisen
- ❖ Verhinderung und Eindämmung von sich abzeichnenden Krisen
- ❖ Stabilisierung, Rückgewinnung und Ausbau von Verständnis, Vertrauen und Glaubwürdigkeit in einer Krise<sup>111</sup>

In dem Beispiel unseres Pharma-Unternehmens ExAmple AG kann man davon ausgehen, dass es tatsächlich Konzepte gibt, wie branchenspezifische Krisen gemeistert werden sollen, oder dass zumindest Kontakte zu PR-Profis bestehen, die wissen, wie man mit Bürgerprotesten zu Tierversuchen und Chemieunfällen umgeht. Für IT-Sicherheitsbeauftragte, Datenschützer und Co. stellt sich das als ein bekanntes Problem dar: Auch im Rahmen der Public Relations konzentriert man sich auf die eigentliche Leistungserbringung des Unternehmens. Und es ist davon auszugehen, dass sich auch die Krisen-PR danach ausrichtet. Im schlimmsten Fall stehen die Pressesprecher im Krisenfall dann im Regen, weil das Sicherheitsteam mit der Abarbeitung der Krise beschäftigt ist, während man sich in den Foren von Heise-Security<sup>112</sup> über die improvisierte und fehlerhafte Pressemitteilung des Unternehmens lustig macht. Um das zu verhindern müssen Sicherheitsexperten auf die Kommunikationsprofis des Unternehmens zugehen und sie mit den nötigen Informationen füttern, die sie zur Bewältigung eines Sicherheitsvorfalls im Rahmen der Öffentlichkeitsarbeit benötigen: Wenn man nicht gerade in einem Unternehmen arbeitet, das Sicherheitsdienstleistungen erbringt, wird man dort auf weitestgehend unbestellte Felder stoßen.

Der erste Schritt in Sachen Security-Krisen-PR besteht also darin Kontakt zur der Abteilung oder den Mitarbeitern aufzunehmen, die mit der Öffentlichkeitsarbeit des Unternehmens betraut sind. Nachdem Sicherheitsexperten im Allgemeinen wenig Erfahrung im Bereich Öffentlichkeitsarbeit haben, sollten sie zunächst Fragen, ob es bereits Vorkehrungen für Sicherheitsvorfälle gibt, wie diese aussehen und ob man mit dem Security-Team bei deren Gestaltung mithelfen kann. In einem solchen Gespräch sollten die folgenden Punkte unbedingt berücksichtigt werden:

- ❖ Sind die wichtigsten Begriffe aus der Security-Welt bekannt?

---

<sup>111</sup> Tanja Köhler; Krisen-PR im Internet: Nutzungsmöglichkeiten, Einflussfaktoren und Problemfelder; 2006; VS Verlag; ISBN: 9783531148984; Seite 75 ff 

<sup>112</sup> <http://www.heise.de/security/foren/>

- ❖ Gibt es vorgefertigte Pressemitteilungen zu gängigen Sicherheitsvorfällen, zum Beispiel Website-Defacements oder Verletzungen des Kunden-Datenschutzes?
- ❖ Sind den PR-Profis alle relevanten Medien mit Security-Bezug bekannt und kennen sie Ansprechpartner in den Redaktionen?
- ❖ Existiert ein auf Sicherheitsvorfälle im Bereich IT und Datenschutz ausgerichteter Presse-Verteiler?
- ❖ Ist bekannt, in welchen Schritten Sicherheitsvorfälle von den IT-Sicherheitsbeauftragten, Datenschützern oder Sicherheitsbeauftragten abgearbeitet werden?
- ❖ Ist bekannt, wer bei Sicherheitsvorfällen für die PR-Profis intern der Ansprechpartner ist und wie die Kommunikation während der Krise laufen soll?

Mit diesen Fragen ist der Grundstein gelegt, um die Kompetenzen der Medien-Profis mit denen der Security-Profis zu einer sinnvollen Krisen-PR zu kombinieren, die dem Security-Team den Rücken frei hält, sich um den eigentlichen Vorfall kümmern zu können. Dadurch kommt der Krisen-PR die Aufgabe zu, über den Vorfall zu informieren und in gewisser Weise vom eigentlichen Geschehen abzulenken. Wenn zum Beispiel einer Zeitung eine CD mit vertraulichen Kundendaten zugespielt wird, gibt es die Möglichkeit auf die Öffentlichkeit zuzugehen, bevor die Artikel der Fach-Medien geschrieben sind, oder erst danach. Im ersten Fall handelt man, während man im zweiten Fall nur noch reagiert. Die Zeitspanne zwischen Handeln und Reagieren ist dabei reichlich kurz. Wenn der Pressesprecher keine Ansprechpartner hat und sich darauf verlässt, die Presse über die Website mit Meldungen zu versorgen, dann kann das natürlich nicht funktionieren, wenn die Website offline ist.

Aber nicht nur extern muss richtig informiert werden. Auch intern gibt es unter Umständen Informationsbedarf. Dies betrifft zuerst den Personenkreis, für den man – wie im vorigen Abschnitt empfohlen – festgelegt hat, dass ihm tiefere Einblicke in den Sicherheitsvorfall zu gewähren sind, aber auch die Mitarbeiter haben einen Anspruch auf Informationen, die über ein knappes „Website offline“ hinaus gehen. Dieser Aspekt der internen Kommunikation greift auch auf den Ratschlag aus Abschnitt 4.6 zurück: *„Tue Gutes und rede darüber.“* Der Sicherheitsvorfall darf im Flurgespräch zwischen den Mitarbeitern nicht zu einem Verriss des Security-Teams werden. Spekulationen darüber, ob man auch *„alles im Griff“* habe, oder *„den Vorfall hätte verhindern können“*, wenn man nur nicht immer *„die Leute mit Bildschirmschonern und abgeschlossenen Türen quälen“* würde, müssen dringend verhindert werden.

Im Grunde hat man intern denselben Mechanismus wie extern: Wenn Menschen keine Informationen aus erster Hand bekommen, müssen sie sich diese

anderweitig beschaffen oder selbst zusammenreimen – beides kann nicht im Sinne der Security-Profis sein. Wenn sich erst einmal die Meinung durchgesetzt hat, dass einem der Sicherheitsvorfall über den Kopf gewachsen ist, ändert das auch keine E-Mail mehr, die darauf hinweist, dass man jederzeit Herr der Lage war.

Zu einer erfolgreichen Krisen-PR gehört daher nicht nur eine funktionierende externe Kommunikation, sondern auch der interne Informationsfluss muss gesteuert werden. Je nach Unternehmensgröße kann man sich bei beiden Aufgaben auf entsprechende Fachabteilungen abstützen, wenigstens bei einer oder man ist ganz auf sich gestellt. Ist das Unternehmen oder die Behörde so klein, dass es keine PR-Spezialisten gibt, kann man auch davon ausgehen, dass die Aufgabe der Krisen-PR an Komplexität abnimmt. In diesen Fällen sollte man sich mit der Geschäfts- und Behördenleitung abstimmen, wie der Kontakt zu lokalen Medien stattfinden soll.

Auch für kleine Unternehmen und Behörden ist es jedoch ratsam für die wahrscheinlichsten Sicherheitsvorfälle interne wie externe Mitteilungen vorzubereiten. Was in der ersten Meldung zu einem Sicherheitsvorfall wirklich nichts verloren hat ist die Aussage, man hätte alles im Griff und das Ausmaß des Schadens sei bekannt! Die folgenden Fragen sollten berücksichtigt werden:

- ❖ Was ist passiert?
- ❖ Wie geht es weiter?
- ❖ Wie lange bleibt das Problem bestehen?
- ❖ Wer ist betroffen?
- ❖ Was ist zu beachten?
- ❖ Wer steht für Fragen zur Verfügung?

Diese Fragen sollten jeweils intern wie extern beantwortet werden. Die Antworten werden dabei unterschiedlich ausfallen, weil die Leser der Meldung auch unterschiedliche Dinge interessieren werden. Das folgende Beispiel aus der ExAmple AG soll diesen Unterschied in groben Zügen verdeutlichen und den Inhalt der Meldung skizzieren:

| Intern                     |                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Was ist passiert?</b>   | Eine unverschlüsselte DVD mit Kunden-Daten wurde entwendet und an eine Zeitung übergeben.                                                                          |
| <b>Wie geht es weiter?</b> | Die Datenschutzbeauftragte Alice hat ihre Ermittlungen aufgenommen und der IT-Sicherheitsbeauftragte Bob die Maßnahmen des Incident Management Guides eingeleitet. |

|                                               |                                                                                                                                                                                                  |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Wie lange bleibt das Problem bestehen?</b> | Weitere Informationen werden nach Abschluss der Schadensanalyse bekanntgegeben, spätestens jedoch im Laufe des morgigen Tages.                                                                   |
| <b>Wer ist betroffen?</b>                     | Nach Aussagen der Zeitung handelt es sich um die Kontodaten aller Kunden der letzten zwei Jahre. Die Datenschutzbeauftragte Alice ermittelt zurzeit den Kreis der tatsächlichen Betroffenen.     |
| <b>Was ist zu beachten?</b>                   | Für die Account-Manager ist das Merkblatt IT-Sicherheits- und Datenschutzvorfälle mit Kundenbezug zu beachten. Aussagen zum Vorfall selbst werden nur durch die Datenschutzbeauftragte getätigt. |
| <b>Wer steht für Fragen zur Verfügung?</b>    | Fragen und Hinweise zum Vorfall können an die Mail-Adresse IncidentManagement@ExAmple.com gesendet werden.                                                                                       |
| <b>Extern</b>                                 |                                                                                                                                                                                                  |
| <b>Was ist passiert?</b>                      | Die XY-Zeitung berichtet in ihrer aktuellen Ausgabe vom Verlust einer DVD mit Kunden-Daten der ExAmple AG.                                                                                       |
| <b>Wie geht es weiter?</b>                    | Der Vorstand der ExAmple AG hat interne Ermittlungen und die Maßnahmen des Incident Management Guides veranlasst.                                                                                |
| <b>Wie lange bleibt das Problem bestehen?</b> | Weitere Informationen werden nach Abschluss der Schadensanalyse bekanntgegeben, spätestens jedoch im Laufe des morgigen Tages.                                                                   |
| <b>Was ist zu beachten?</b>                   | Die Öffentlichkeit wird umgehend über den Verlauf der Schadensanalyse informiert.                                                                                                                |
| <b>Wer steht für Fragen zur Verfügung?</b>    | Konkrete Fragen zum Sachverhalt können an die Mail-Adresse IncidentManagement@ExAmple.com gesendet werden.                                                                                       |

**Tabelle 5-5:** Beispiel zur Krisen-PR

Die Beantwortung der Fragen hängt für Ihren konkreten Fall natürlich von einigen zusätzlichen Parametern ab, wie zum Beispiel die allgemeine Informationspolitik des Unternehmens oder der Behörde. Wenn man sich jedoch für eine offene Informationspolitik entscheidet, dann sollten die Meldungen verdeutlichen, dass das Thema ernst genommen wird und man sich der Sache professionell annimmt.

Außerdem sollte sie Zeit verschaffen, sich Detailmeldungen genauer überlegen zu können. Was in jedem Fall vermieden werden muss, sind Aussagen, von denen man befürchten muss, sie hinterher wieder dementieren zu müssen.

## 5.5 Wenn die Unterstützung von höchster Stelle fehlt

Eine Krise der besonderen Art: Dem Security-Personal fehlt jegliche Unterstützung von höchster Stelle. Im besten Falle sind die Entscheidungsträger zu Lippenbekenntnissen bereit. Eine Situation, aus der die Betroffenen nur mit größter Mühe wieder herauskommen. Wer sich aus dieser Situation freikämpfen will, muss sich auf eine langfristige Strategie einlassen: Ein klärendes Vier-Augen-Gespräch wird sicher nicht die Kehrtwende bringen. Die Ausgangssituation ist eigentlich gar nicht so schlecht. Die Studie *„Sicher – von oben“* stellt fest<sup>113</sup>, dass die befragten Chefs in einer ersten Reaktion, über alle Branchen, Firmengrößen und Positionen hinweg, einhellig bekräftigen: *„Ein Zuviel an Sicherheit kann es gar nicht geben.“* Leider sind sich die Chefs genauso einig, dass die eigenen Sicherheitsmaßnahmen – im Unternehmen wie auch privat – ausreichend sind.

*„Nie genug“, „genug“* – Was denn nun? Das Problem scheint zu sein, dass man Führungskräften in den letzten Jahren beigebracht hat, allen ihren Mitarbeiter zu sagen, dass sie der Mittelpunkt der Welt seien – unwichtige oder weniger wichtige Mitarbeiter gibt es in Unternehmen nicht mehr – zumindest wir das nicht zum Ausdruck gebracht. Dadurch entsteht Raum für Missverständnisse. Man kann davon ausgehen, dass dieselben Chefs in einer Studie über Marketing verkünden, dass man nie zu viel Werbung machen kann und in einer Studie über den Vertrieb, dass nie zu viel akquiriert werden kann usw. Im zweiten Satz folgt dann sogleich die Einschränkung – der allseits bekannte Zweiklang der modernen Führungskraft: Zunächst loben und bestärken und erst dann in die Pfanne hauen. Daher sollte man sich nicht an jeden Strohalm klammern, der einem in Form eines Lobs hingehalten wird – interessanter ist das, was nach dem Strohalm kommt.

Auch in der genannten Studie wird der Strohalm schnell weggezogen und die eigentliche Einstellung zum Thema vorgebracht:

- ❖ Sehr komplizierte Genehmigungsverfahren
- ❖ Lange Zeitdauer
- ❖ Hohe Kosten

---

<sup>113</sup> known\_sense (Herausgeber u.a.); Sicher – von oben: Qualitative Imageanalyse CISO & Co. Security Manager und Informationssicherheit aus Sicht von Geschäftsführung, Management und Vorständen; 2009; known\_sense; Seite 21 ff

- ❖ Langwierige Diskussionen
- ❖ Neue Kommunikationsmöglichkeiten sind nicht erlaubt.
- ❖ Sicherheitsstandards schließen die erwartete und gewünschte Flexibilität und Kundenorientierung mitunter aus.

Chefs fühlen sich in der eigenen Tätigkeit eingeschränkt, obwohl sie genau wissen, dass diese Einschränkungen durch Sicherheitsstandards sinnvoll sind und sie sogar konstatieren, dass man gar nicht sicher genug sein kann.

IT-Sicherheitsbeauftragte, Datenschützer und Co. sollten daher einen Filter über diese Aussagen legen und die konflikträchtigen Anteile herausarbeiten. Nur so erfahren sie, wo den Chefs eigentlich der Schuh drückt. Wenn man dann die Zeit, in der sie sich mit Sicherheit beschäftigen und die Zeit, in der sie andere Sachen machen ins Verhältnis setzt, weiß man, wo man eigentlich steht. Für viele könnte diese Sichtweise ziemlich ernüchternd ausfallen. Nehmen wir ein Beispiel:

- ❖ Sprechzeit beim Chef: 5 Stunden pro Quartal
- ❖ Negative Aussagen des Chefs:
  - „Riesenprobleme“
  - „total nervige Prozesse“
  - „sicher ist nur der Tod“

Wenn die Unterstützung von höchster Stelle fehlt, bleiben bei dieser Ausgangssituation nur zwei Stellschrauben am Verhältnis zum Chef. Dazu gehört nicht, dass man nach mehr Anerkennung sucht. Für Sicherheitsprofis in dieser schwierigen Situation gilt: Ein Tag ohne Gegenwind ist Lob genug.

**Die erste Stellschraube** ist also, die negativen Aussagen zu reduzieren und sie dahin umzuleiten, wo sie hingehören: Zu den Leuten, die Entscheidungsträgern immer wieder die sprichwörtlichen Flöhe ins Ohr setzen. Wenn sichere Prozesse als nervig und zeitraubend empfunden werden, muss den Chefs ja irgendwer unsichere Prozesse vorgestellt haben, die nicht nerven und schneller gehen. Das waren aber leider nur leere Versprechungen. Chefs sollten sich über die Personen ärgern, der ihnen leere Versprechungen machen und nicht über die, die ihnen reinen Wein einschenken. Wann immer ein Entscheidungsträger eine Einschränkung durch eine Sicherheitsmaßnahme ins Visier nimmt, muss die Frage aus dem Security-Team lauten: *„Wer hat Sie denn da wieder ins offene Messer laufen lassen und erzählt, dass ginge auch alles schneller? Da hat Ihnen wohl wieder jemand das Manna vom Himmel versprochen ohne sich vorher zu informieren.“*

Bevor Sie jedoch einen Chef auf diese Art in die Enge treiben, sollten sich im Klaren darüber sein, dass die bereits zitierte Studie *„Sicher – von oben“* ebenso gezeigt hat, dass es in der Beziehung zwischen Chefs und Sicherheitsprofis auch

um die Frage von Kontrollverlusten geht. Chefs wollen und müssen ihre Position wahren und reagieren sehr sensibel auf Machtdemonstrationen aus der Security-Ecke. Sie sollten Ihren Chef also keinesfalls öffentlich so angehen und müssen die Botschaft möglicherweise in Watte packen und mit Engelszungen überbringen. Dabei muss herausgearbeitet werden, dass man die Machtposition des Chefs niemals in Frage stellen würde. Im Gegenteil: Man macht loyal darauf aufmerksam, dass jemand der dem Chef unausgegorene, unsichere Ideen unterjubelt offensichtlich keine Angst hat, dabei erwischt zu werden.



**Abbildung 5-5:** Leiten Sie den Ärger des Chefs dahin, wo er hingehört

**Die zweite Stellschraube** betrifft die Zeit: Die Security-Zeit muss signifikant gesteigert werden. Das betrifft insbesondere die Zeit, in der Security als Lösung und nicht als Problem gesehen wird. Dazu muss nicht nur mehr Zeit beim Chef verbracht werden; es muss zusätzlich jede Möglichkeit genutzt werden, dort mit funktionierenden Dingen und Lösungen aufzutauchen. Viele Security-Profis versuchen ihren Chefs den Rücken frei zu halten, indem sie dort nur auftauchen, wenn es Schwierigkeiten oder Ärger gibt. Bei den Chefs bleibt von den vielen schlechten Nachrichten irgendwann auch etwas an der Person des IT-Sicherheitsbeauftragten oder des Datenschützers hängen. Wir haben diesen Punkt bereits im Abschnitt 4.6 (Tue Gutes und rede darüber) näher beleuchtet.

Ein guter Ansatzpunkt scheint es zu sein, sich den Chefs als Ansprechpartner in Sicherheitsfragen des privaten Lebens anzubieten. Die berufliche Auseinandersetzung mit den Gefahren der modernen Kommunikationstechnik führt auch privat zu einer höheren Sensibilität und einem veränderten Umgang

mit den eigenen sensiblen Daten.<sup>114</sup> Gerade was das Internet-Verhalten der Kinder angeht kann man so sicher wertvolle Gespräche führen, die beim Chef gut in Erinnerung bleiben.

## 5.6 Zusammenfassung

Für Sicherheitsprofis besteht immer die Gefahr in der Buhmann-Falle zu landen und als Überbringer der schlechten Nachricht ins Visier von Anfeindungen zu geraten. Das lässt sich nicht gänzlich verhindern, kann mit der richtigen Strategie jedoch auf ein Mindestmaß reduziert werden. Wie schon in den vorherigen Kapiteln spielen auch hier die kommunikativen Fähigkeiten der Protagonisten eine entscheidende Rolle. Einmal mehr werden die Soft-Skills der Sicherheitsprofis zum Schlüssel zum Erfolg.

Das zuletzt behandelte Problem, mit dem sich einige Sicherheitsprofis auseinander setzen müssen, ist zugleich das schwerwiegendste, weil es sich auf alle anderen Probleme, Schwierigkeiten und Konflikte des Security-Alltags auswirkt. Daher ist es nur verständlich, dass sich diese Situation nur bekämpfen lässt, wenn man die geballte Ladung an Möglichkeiten mobilisiert, die in diesem Buch vorgestellt wurden. Auch, wenn Sie in dieser schwierigen Situation festsitzen: Es gibt einen Ausweg aus der Buhmann-Falle und er führt über mehr und bessere Kommunikation: Zum Beispiel mehr Kommunikation mit Branchenkollegen oder dem Betriebsrat und bessere Kommunikation durch ein gemeinsames Vokabular. Mehr Kommunikation durch den gezielten Ausbau von Awareness-Maßnahmen und bessere Kommunikation durch die Übersetzung der eigenen Ziele in die Problemfelder der Personengruppe, mit der man gerade arbeitet. Mehr Kommunikation über die eigenen Erfolge und Leistungen und bessere Kommunikation durch mehr Konzentration auf den Risikofaktor Mensch.

---

<sup>114</sup> known\_sense (Herausgeber u.a.); Sicher – von oben: Qualitative Imageanalyse CISO & Co. Security Manager und Informationssicherheit aus Sicht von Geschäftsführung, Management und Vorständen; 2009; known\_sense; Seite 26

## 6 Am Ende kommt der Applaus

*„Ich habe das Geheimnis des Erfolgs gefunden:  
Fehler, Fehler und noch mehr Fehler, aber weniger, weniger und immer weniger.“  
Ogden Nash, 1902*

Auf der Security-Bühne wie im echten Leben, erst am Ende der Vorstellung kommt der Applaus. Auch wenn es zwischendurch manchmal Szenenapplaus gibt, wie das Publikum am Ende reagiert weiß man nie genau. Mit etwas Glück und einem geneigten Publikum schafft man es vielleicht sogar zu Standing Ovationen. Eines steht jedenfalls fest: Der Weg dorthin ist für Sicherheitsexperten jedenfalls steinig. Alice, Bob und Dave aus der ExAmple AG haben ihn jedenfalls redlich verdient.



**Abbildung 6-1:** Standing Ovationen für die Sicherheitsprofis

Ganz gleich, ob Sie in Ihrem Unternehmen oder Ihrer Behörde für IT-Sicherheit, Datenschutz oder allgemeine Sicherheitsfragen verantwortlich sind; ob Sie als Unternehmensberater oder auch ganz anders mit dem Thema Sicherheit zu tun haben – ich hoffe, dass Ihnen das vorliegende Buch als Wegweiser und kleine Hilfe dienen wird, den beruflichen Alltag auf der Security-Bühne frei von unnötigen Konflikten zu meistern.

## 6.1 Leitsätze zum Konfliktmanagement

Die letzte Frage, mit der sich dieses Buch befassen soll, ist die Frage nach zehn kurzen Formeln, auf die sich die Aussagen, Ideen und Denkanstöße dieses Buchs bringen lassen.

### 6.1.1 Satz 1 – Problemfelder

Alle Sicherheitsanstrengungen müssen sich an den Problemfeldern (Zwänge, Ziele, Prioritäten und Risiken) der Mitarbeiter und Chefs ausrichten.

Nur wenn sich die Sicherheitsexperten an den Problemen der Mitarbeiter und Chefs und den Schwierigkeiten der Fachabteilungen orientieren, werden sie ihre Botschaft vermitteln können. Die Botschaft muss nicht objektiv für den Sender einen Sinn ergeben – was zählt ist, dass sie subjektiv für den Empfänger einen Sinn ergibt.

### 6.1.2 Satz 2 – Nur im Team

IT-Sicherheitsbeauftragte, Datenschutzler und Co. müssen zusammenarbeiten.

Die unterschiedlichen Security-Disziplinen müssen ein gemeinsames Ziel entwickeln und gemeinsam daran arbeiten es voran zu bringen. Wenn sich die verschiedenen Sicherheitsbeauftragten gegenseitig im Weg stehen, werden sie auch von außen keine Unterstützung für ihre Arbeit bekommen.

### 6.1.3 Satz 3 – Kommunikation ist Alles

Nur wer sich verständlich ausdrückt, hat Anspruch darauf, Gehör zu finden. Konfliktpräventive Kommunikation ist...

- ❖ klar,
- ❖ treffend,
- ❖ knapp,
- ❖ wertfrei und
- ❖ konstruktiv.

Konfliktpräventive Kommunikation ist für IT-Sicherheitsbeauftragte, Datenschutzler und Co. der Grundstein für einen Arbeitsalltag, der frei von unnötigen Konflikten ist. Sie bewahrt davor, in unnötige Randgefechte und persönliche Konflikte abzudriften.

### 6.1.4 Satz 4 – Der Mensch

Im Mittelpunkt jeder Sicherheitsbetrachtung steht menschliches Handeln und Unterlassen. Bewusst oder unbewusst: Der Mensch ist der Risikofaktor Nummer 1!

Wie man es auch dreht und wendet – es läuft immer darauf hinaus, dass ein Mensch etwas getan oder unterlassen hat. Auch technischem Versagen ist immer eine menschliche Fehlentscheidung vorangegangen: Zu wenig Stabilität, zu wenig Redundanz oder einfach eine falsche Risikoeinschätzung.

### 6.1.5 Satz 5 – Die Technik

Technische Sicherheitsmaßnahmen können nie eine abschließende Antwort auf Risiken sein, die auf ein sozio-technisches Gesamtsystem einwirken.

Informationssysteme sind sozio-technische Gesamtsysteme, die aus Informationen, Hardware, Software und aus den beteiligten Menschen bestehen. Sicherheitsmaßnahmen müssen sich folglich aus dem Gesamtsystem ableiten und aufeinander abgestimmte, soziale sowie technische Komponenten enthalten.

### 6.1.6 Satz 6 – Gemeinsames Vokabular

Sicherheitsprofis sind von einem Begriffsdschungel umgeben, der Missverständnisse geradezu provoziert. Zu Beginn jeder Zusammenarbeit muss man sich auf ein gemeinsames Vokabular verständigen.

Zum dritten Mal in diesem Buch die Frage: Was war noch schnell der Unterschied zwischen IT-, IV-, IS- und I-Sicherheit? Oder Funktionssicherheit, Betriebssicherheit, Datensicherheit, Datensicherung, Informationssicherheit, Safety, Protection, Security, Privacy, Datenschutz usw.? Ohne die Verständigung auf gemeinsame Begriffe leben Sicherheitsexperten im modernen Babylon.

### 6.1.7 Satz 7 – Marketing

Der gezielte Einsatz von guten und schlechten Nachrichten und ein konsequentes Selbstmarketing sind für die Außenwahrnehmung von IT-Sicherheitsbeauftragten, Datenschützern und Co. entscheidend.

Wenn die Sicherheitsexperten keine Werbung für sich machen, dann macht es garkeiner. Das richtige Marketing für die eigene Sache verhindert, dass sie frustriert in der Buhmann-Falle landen.

### 6.1.8 Satz 8 – Motivation

Großes Augenmerk muss darauf gelegt werden, Mitarbeiter, Chefs und nicht zuletzt sich selbst zu motivieren. Motivierte und aufmerksame Menschen sind besser, wie jedes Intrusion Detection System.

Technische Sicherheitslösungen gibt es, und man kann Sie überall kaufen. Motivierte Mitarbeiter und Chefs sind durch kein Geld der Welt zu ersetzen. Es geht sogar darüber hinaus: Mit motivierten Mitarbeitern und Chefs wird man mehr Spielräume für technische Lösungen haben und so insgesamt – und eben auch technisch – besser dastehen.

### 6.1.9 Satz 9 – Neue Ideen

Den Angreifern gehen die Ideen nicht aus, wie sie die Menschen dazu bringen, das zu tun, was zu ihrem eigenen Vorteil ist. Die Verteidiger werden auf Dauer nur erfolgreich sein, wenn sie sich eine ebensolche Kreativität aufbauen, erhalten und mit immer neuen Ideen kontern.

Viele technische Sicherheitslösungen sind weitestgehend ausgereift. Sicherheitslücken entstehen entweder durch Fehlkonfigurationen oder durch menschliche Fehlleistungen. Die Möglichkeiten am Risikofaktor Mensch anzusetzen, sind noch weitestgehend ungenutzt.

### 6.1.10 Satz 10 – Erfolg

Der Erfolg als Sicherheitsprofi hängt mehr von den kommunikativen Fähigkeiten ab, als von den technischen. Informationssicherheit, Datenschutz und IT-Sicherheit sind Management-Aufgaben.

Sicherheitsprofis, die den Begriff Informationssystem auf seine technischen Aspekte beschränken und nicht als sozio-technisches Gesamtsystem begreifen, werden immer wieder an Grenzen stoßen und sogar damit Probleme haben, technische Maßnahmen durchzusetzen.

Mit einem Sachwortverzeichnis kann man verschiedene Ziele verfolgen. Das Hauptziel ist es, ein Nachschlagen von Sachwörtern zu ermöglichen. Ein anderes Ziel kann es sein, Lust zu machen, an einer bestimmten Stelle nachzuschlagen, ein weiteres, eine Stelle wiederzufinden, an die man sich nicht mehr richtig erinnern kann. Daher enthält diese Sachwortverzeichnis auch die Begriffe, die auf den ersten Blick nichts mit Security-Konflikten zu tun haben, an die Sie sich nach dem Lesen aber vielleicht noch erinnern können – wundern Sie sich daher nicht über die Sachworte *Reis*, *Nudeln* und *trocken Brot*.

## Sachwortverzeichnis

11.09.2001 16

### A

Abgrund 167

Abhängigkeit 41

Administrator-Rechte 41

Adware 41

Akquise-Bühne 32

Akt, erster 141

Akt, zweiter 143

Alice 26, 27, 28, 29, 57, 58, 59, 102, 103,  
133, 134, 135, 137, 138, 139, 140,  
148, 149, 150, 162, 168, 170, 177,  
178, 183

Alien 17, 143

Amenpanufer 15, 53

Anfangsphase 83

Angebotsunterlage 30, 45

Angst 18, 56, 115

antiautoritäre Erziehung 42

Anual Loss Expectancy 31

Äpfel 85

Applaus 183

Arbeitssicherheit 13

Archimedes 125

Atommodell 64

Augias 148

Authenticity 73

Autor 6

Availability 74

Avatare 145

Awareness-Kampagne 106

### B

Bad Cop 130

Beeinträchtigung 41

Bestellung 52

Besuchergruppe 86

Betriebsrat 21, 36, 51

Betriebsvereinbarung 26

Bevormundung 45

Beweggründe 9

BGB 19

Black-Box 100

blackhat 154

Blockbuster 32

Bob 26, 27, 28, 29, 57, 58, 59, 69, 102,  
103, 111, 133, 134, 135, 137, 138,  
139, 140, 148, 149, 150, 151, 162,  
163, 168, 170, 177, 183

Botschaft 23  
Brainstorming 135  
BruCON 155  
BSI 22, 32, 78, 98  
Bühne 5  
Bundesarbeitsgericht 51  
Bundesdatenschutzbeauftragter 20  
Bundesnachrichtendienst 69  
Bundeswehr 12  
Bürogeräteaum 30

## C

certainty 72  
charmante Gauner 48  
Chef 8, 92, 129, 179  
Chinesische Mauer 15  
CISO (im ganzen Buch)  
Confidentiality 74  
Cool 152  
Corporate Security 79

## D

Datenschutz 13, 25, 74  
Datenschutzbeauftragte (im ganzen Buch)  
Datenschutzgesetz 19, 21  
Datenschutzmanagement 78  
Datensicherheit 72  
Datenverarbeitungsgesetz 20  
Dave 26, 27, 28, 29, 30, 31, 32, 45, 46, 57, 58, 59, 67, 86, 87, 102, 103, 111, 133, 134, 135, 137, 138, 139, 140, 148, 149, 150, 168, 183  
Debatte 166  
Deeskalation 67, 81  
Def Con 154  
Default Policy 63

Demaskierungen 166  
Dialogphase 84  
Dienstleistung 46  
Dienststellenleiter 8  
Dilemma 59  
Diskretion 170  
Diva 9  
Dornröschenschlaf 16  
„drive-by“-Risikoaanalyse 33, 35, 53, 114  
Drohkulisse 164  
Drohstrategien 166

## E

EDV-Fachkraft 51  
egoistischen Individualisten 48  
Ehevertrag 55  
Eigenkapitalgeber 11  
Eigenmotivation 118  
Einstiegsphase 83  
Eintrittswahrscheinlichkeit 31  
Einverständniserklärung 21  
Empfänger 23  
Endphase 86  
Entscheidungsfreiheit 45, 58  
Erfolg 186  
Eskalation 81, 161  
Eskalationsstufen 164  
Etikettenschwindel 22, 24  
ExAmple AG 26, 27, 30, 50, 57, 67, 69, 86, 101, 102, 103, 108, 110, 133, 134, 138, 139, 148, 149, 150, 162, 168, 169, 170, 175, 177, 178, 183

## F

Fallbeispiel 26, 28, 30, 45, 50, 57, 86, 101, 102, 103, 133, 137, 138, 148, 162, 168

Faust (Goethe) 20, 34  
Fax 30, 45  
Feuerwehr 13  
Filme, anzügliche 170  
Filmliste 152  
Fliege 111  
Flucht in einfache Tätigkeiten 24  
Flugangst 117  
Flughafen 111  
Freiheit 19  
Frustration 118  
Führungsgrundsätze 41  
Fünf-Schritte-Modell 161

## G

Gebranntes Kind 93  
Gefahr 55  
gelebte Praxis 48  
Gemeinschaft 55  
gemischtes Eis 52, 59  
General Meng-tian 15, 141  
Geringschätzung 44  
Geschäftsführer 8  
Gewinnmaximierung 9, 10, 11  
Girolamo Savonarolas 136  
Good Cop 130  
Google Hacking 94  
Google Hacking Database (GHDB) 94  
Gouthier 46

## H

Hacking for Beer 155  
Handeln 90  
Handlung 16  
Handlungssicherheit 33  
Handlungsspielraum 41

Handschlag 55  
HB-Männchen 145  
Hebel 125  
Heilen 62  
Held 6, 14  
Herkules 148  
Herzberg 91  
Hippokrates 61  
Hollywood 17, 143  
Holzhammermethode 43  
homo carens securitate 111  
homo oeconomicus 110  
Hygienefaktoren 90

## I

ICE 31  
Ideen 186  
Impfung 81  
Improvisation 33  
Information 68  
Informationssicherheit 21, 74  
Informationssicherheitsbeauftragte (im ganzen Buch)  
Informationssicherheitsmanagement (im ganzen Buch)  
Informationssystem 68  
Informationssystemssicherheit 21  
Innovationspotential 49  
Integrity 74  
Interessen 41, 54  
Interessenkonflikt 15, 50  
Interessenvertretung 36  
I-Sicherheit 77  
IS-Sicherheit 77  
IT-Grundschutz 22, 32, 35, 117  
IT-Sicherheit 13, 26, 76

IT-Sicherheitsbeauftragte (im ganzen Buch)

IV-Sicherheit 76

## K

Kanonen 161

Kartoffeldiagramm 25, 26, 27, 38

Kaufhaus 20

<kes> (Zeitschrift) 21

Kissinger, Henry 159

klar 63

knapp 63

Koalitionen 166

Kommunikation (im ganzen Buch)

Kommunikation, systemische 136

Kommunikationskrone 66

Kompetenzüberschreitung 22

Konflikt 40, 81

Konfliktamplitude 81

Konfliktdauer 81

Konflikt-Falle 39

Konflikt-Monitoring 168

Konflikt-Phasen 165

Konfliktpipeline 81

konfliktpräventive Kommunikation 63

Konfliktvoraussetzungen 40

konforme Mitarbeiter 48

konstruktiv 66

Kontrollfunktion 52

kreativen Individualisten 48

Kreativität 57

Krisenbewältigung 159

Krisen-PR 174

Kultur-Förderung 32

Kundenbeziehung 49

## L

Laie 31

Landkarte 28, 44

Leitsätze 184

Lenkung 45

Linienorganisation 22

Live 94

Lochkartenmaschine 9

Lose-Lose 165

Lösungsphase 85

Lust-Frust-Bilanz 120

## M

Manipulation 90

Marketing 33, 156, 185

Mauer des Schweigens 171

Mausefalle 1

Meinungsverschiedenheit 40

Mensch 185

Metadaten 95

Mietvertrag 55

Mietwagen 55

Militär 13

Misstrauen 18, 55

Missverständnis 18, 19, 22, 23, 28, 68, 72, 78

Mitarbeiter 28, 103

Mitnick, Kevin 65

Motivation 88, 89, 186

Motivatoren 90

Musketiere, drei 25, 26

## N

Nachrichten, negative 135

Nachrichten, positive 131

Nadelöhr 104

Nash, Odgen 183

Nebenjob 51, 53

Networking 119

Non Repudiation 74

Normenkreuz 46, 49

Nudeln 22

## O

OnlinePLUS-Service 4, 28, 38, 57, 96,  
120, 131

Outsider 48

## P

Passwort 41

Patch-Day 133

Pawero 15, 141

PDF-Datei 110, 112

PDF-Dateien 95

Pen-Tests 98

Personalrat 36

Personalunion 51

Personalvertretung 36

Pharao Ramses IX 15, 53

Phasenverlauf 16

Phasenverlauf (Awareness) 107

Phasenverlauf, Storyboard 141

Phishing 96

Polizei 13

Potential-Übersicht 121

PR 174

Prävention 61

Prioritäten 8, 15, 26, 28, 34, 37, 90

Privacy 72

Privatvorstellung 37

Problemfelder 15, 20, 22, 26, 28, 34, 35,  
37, 41, 90, 184

Protection 73

Provisorium 33

Prozente 89

Prozesse, geschäftskritische 32

Prozessmodellierung 22

Publikum 6, 28

## Q

Qin Shiuangdi 15, 141

## R

Randnormen 47

Raubritter 16

Regeln 41

Regie 23

Regisseur 6, 7, 14, 32

Reis 23

Retter in der Not 17

Rinder 148

Risiken 8, 15, 26, 28, 34, 37, 90

Risikomanagement 22

## S

Sachwortverzeichnis: Sie suchen  
hoffentlich nicht wirklich im  
Sachwortverzeichnis nach dem  
Begriff Sachwortverzeichnis ;-)

Safety 72

Sanktionen 164

Scheidung 35, 56

Schiphol 111

Schließzylinder 16

Schlüsselnormen 47

Schluss-Szene 17, 143

Schuldige 9

Schuldzuweisung 24

Schulz von Thun 43

Schupse 109

Security 73

Security by 126  
Security-Stammtisch 146  
Security-Storyboard 141  
Sicherheit 13, 25, 55, 56, 71  
Sicherheit, echte 56  
Sicherheit, gefühlte 18, 56  
Sicherheit, tatsächliche 18  
Sicherheitsbeauftragte (im ganzen Buch)  
Sicherheitsbegriff 13, 22  
Sicherheitsbemühungen 25  
Sicherheitsbudget 24  
Sicherheitskultur 32  
Sicherheitspräfixe 76  
Sicherheitsrichtlinien 33  
Sicherheitsrisiko Mensch 24, 41  
Sicherheitsüberprüfung 14  
Sicherheitsvokabular 74  
sozio-technisches Gesamtsystem 70  
Spaß am Job 118  
Spatzen 161  
Spezialisierung 13  
Spionageabwehr 14  
Spyware 41  
Standing Ovations 183  
Stärken 157  
Stellschrauben 180  
Steuerzahler 113  
Streit 40  
Stress 34  
Südkorea 31  
Synonyme 72  
System 69  
System, automatisches 114  
System, kognitives 114

System, reflektierendes 114  
Szenarien 94, 97

## T

Tal der Könige 15  
TANs 115  
Taten statt Worte 166  
Team 184  
Team-Bildung 62  
Technik 70, 185  
Teufel 92  
Toilette 111  
Totenkopf 172  
Totschlag-Argument 31  
Tragödie 20  
Traualtar 55  
treffend 64  
Treueversprechen 55  
trocken Brot 52, 59  
Trojaner 41  
Tür-Falle 96

## U

Unterlassen 90  
Unternehmensphilosophie 41  
Unternehmenssicherheit 79  
Unterstützung 57  
Urheberrecht 172

## V

Verantwortliche 8  
Verantwortung 24, 130  
Verhaltenskreuz 43, 49, 58, 135  
Verhärtung 166  
Vernichtungsschläge 166  
Versetzung 138  
Vertrag 55

Vertrauen 18, 54, 56

Vertrauensverlust 54

Vertrieb 33

Verwirklichung 41

Vokabular 67, 185

Vollzugsbeamte 19

Vorbeugen 62

Vorfälle 17, 141

Vorstand 8

## **W**

Wachschutz 14

Wahnsinn, alltäglicher 17, 141

Wareneinkauf 33

Wayback-Machine 95

Werkschutz 13

wertfrei 64

Wertschätzung 44, 58

White-Box 100

Widerstand 160

Widerstandsklasse 16

Wikipedia 68

Win-Lose 165

Win-Win 165

Wochenmarkt 85

World Trade Center 16

## **X**

XING 39

## **Z**

Zersplitterung der Existenzgrundlagen  
167

Zertifizierung 133

Ziele 8, 12, 14, 26, 28, 34, 37, 41, 90

Zielkonflikt 19

Zielvereinbarungsgespräch 34

Zuse Z1 9

Zuverlässigkeit 51

Zwänge 8, 12, 14, 26, 28, 34, 37, 41, 90

Zwei-Faktoren-Theorie 91

„Zweit-Job-Falle“ 51, 59