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.

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

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

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[1] damit befassen, wie man den Mensch dazu bringt, gegen Sicherheitsregeln zu verstoßen, gibt es nur wenige Bücher[2], 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-Webservers. 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.

---

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

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

Inhaltsverzeichnis

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.[3] In den meisten Fällen stand die Tätigkeit nicht einmal auf dem Berufswunschzettel.[4] 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

---

[3] Frei nach Egmont Colerus, der den Vergleich für die Mathematik benutzt; Vom Einmaleins zum Integral; 1947; Zsolnay; ASIN: B0000BH6NV

[4] 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 umschifft 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[5]

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

[5] 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.

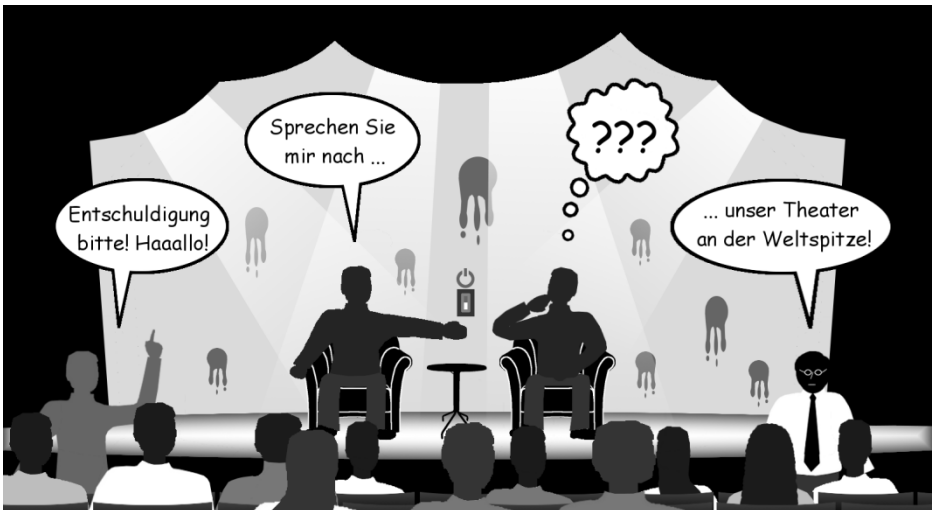

Abbildung 1-2: Das Chaos auf der Security-Bühne ist fast perfekt

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.

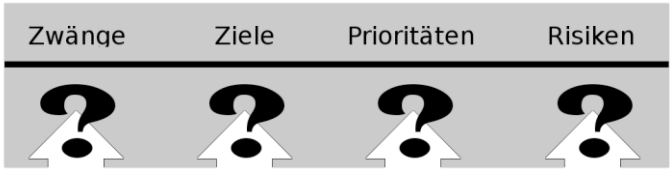

Abbildung 1-3: Die vier Problemfelder der Akteure

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*[6]. 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

---

[6] 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.

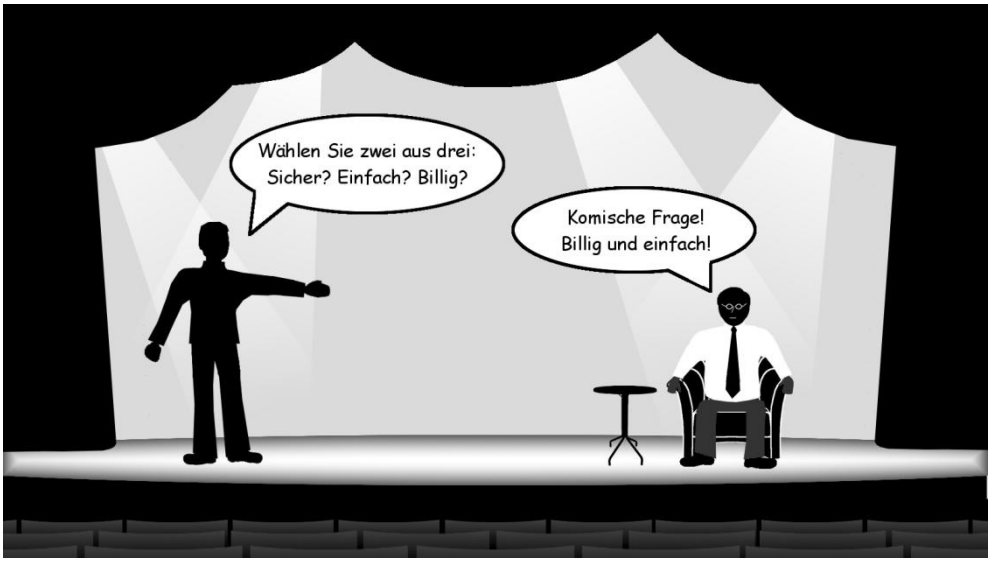

Abbildung 1-4: Die Zwei-Aus-Drei-Entscheidung

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