

Konfliktmanagement für Sicherheitsprofis

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

Gekürzter und überarbeiteter Auszug aus dem
gleichnamigen Buch von Sebastian Klipper.

Das Buch ist erschienen im Vieweg+Teubner Verlag:

<http://www.viewegteubner.de/tu/Konfliktmanagement>

ISBN: 978-3834810106

Der Autor ist selbstständiger Information Security Consultant (CISSP®, T.I.S.P. ®).
Sein Blog „Klipper on Security“ finden Sie unter <http://blog.psi2.de>.

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 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.¹

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 sind die Protagonisten von vier Problemfeldern beeinflusst: Zielen, Zwängen, Prioritäten und Risiken. Wir wollen in diesem Auszug aus „Konfliktmanagement für Sicherheitsprofis“ darauf eingehen, wann es sich formal um Konflikte handelt, und nach welchen Gesetzmäßigkeiten sie entstehen. Am Ende dieses Probekapitels ist dann das Handwerkszeug zusammen, um als Sicherheitsexperte Security-Konflikte verhindern zu können.

Wir werden uns dazu 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 3.) – ursprünglich gar nicht für die Security-Branche entwickelt. Man merkt jedoch schnell, dass sie gute Arbeit leisten, die Probleme zu verstehen, denen man sich als Datenschutz- oder IT-Sicherheitsbeauftragter stellen muss.

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 aber am meisten interessiert: Was im Speziellen sind Security-Konflikte? Diesen Fragen werden wir nun auf den Grund gehen.

Bevor man eine Meinungsverschiedenheit als Konflikt bezeichnet, müssen einige Voraussetzungen erfüllt sein. Konflikte drehen sich immer um eine gewisse Anzahl voneinander abhängiger Personen, deren gegensätzliche Interessen, und den Willen diese durchzusetzen.

¹ <https://www.xing.com/app/forum?op=showarticles;id=7816814>; eingesehen am 14.09.2009; archiviert unter <http://www.webcitation.org/5jmSZadZX>



Abbildung 1: Konfliktsituation: Ein Akteur beeinträchtigt die Interessen des anderen.²

Man spricht von einem Konflikt, wenn eine Interaktion zwischen mindestens zwei Akteuren die folgenden Merkmale aufweist³:

- ❖ 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. 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

² Nach einer Zeichnung von Klaus Puth in: Regina Mahlmann; Konflikte managen: Psychologische Grundlagen, Modelle und Fallstudien; 2001; Beltz; ISBN 9783407363893; Seite 76

³ Regina Mahlmann; Konflikte managen: Psychologische Grundlagen, Modelle und Fallstudien; 2001; Beltz; ISBN 9783407363893; Seite 18

Zugangsdaten – my home ist my castle! So wie wir unseren privaten Computer 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: 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 schließlic 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. 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 Ceedo⁴. 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. Verhaltenskreuz nach Schulz von Thun

Diese Einleitung hat mehr Fragen aufgeworfen, als sie 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 Verhaltenskreuz⁵ vor, das uns bei der Suche nach einer Richtung als Landkarte dienen soll. Unser erster Schritt dabei ist, unseren Standort zu bestimmen.

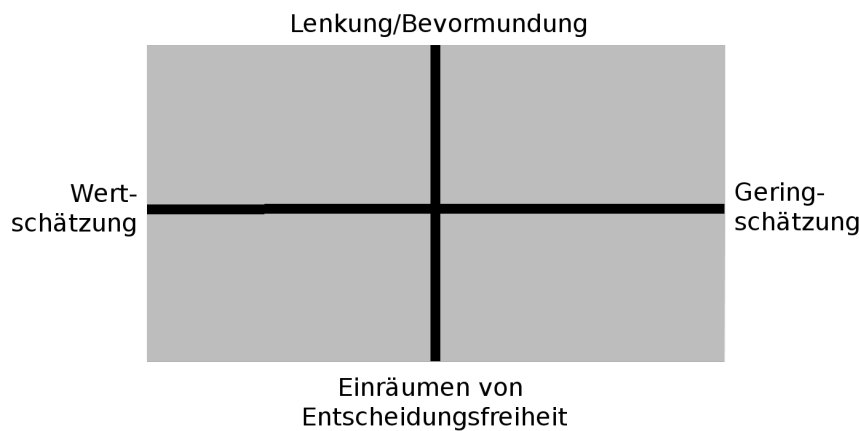


Abbildung 3: Verhaltenskreuz nach Schulz von Thun

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.

⁴ 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.

⁵ Friedemann Schulz von Thun; Miteinander reden 1 - Störungen und Klärungen. Allgemeine Psychologie der Kommunikation; 1981; Rowohlt Taschenbuch Verlag; ISBN: 3499174898; Seite 162 ff

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.

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 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!

Fallbeispiel: Das Angebots-Fax

Einzelne Äußerungen lassen sich in der emotionalen, sowie der Lenkungsdimension im Verhaltenskreuz einschätzen. Als Beispiel greifen wir auf ein Fallbeispiel aus einem anderen Kapitel im Buch zurück. Der Sicherheitsbeauftragte Dave *„erwischt“* darin 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 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.

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. Gouthier⁶ hat ursprünglich zur Beschreibung von Kundenbeziehungen ein Normenkreuz eingeführt, das 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

⁶ Matthias H. J. Gouthier, Bernd Strauss; Kundenentwicklung im Dienstleistungsbereich; 2003; Gabler; ISBN 3824476754; Seite 48

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. 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):

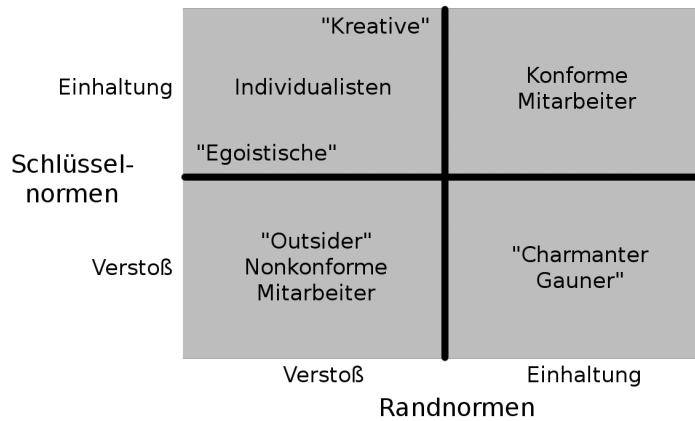


Abbildung 5: Normenkreuz nach Gouthier

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 kurz verlässt. Je nachdem, ob sich ein Mitarbeiter an die Normen hält oder nicht, kann man unterschiedliche Arbeitertypen identifizieren.

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.

In der folgenden Tabelle 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.

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

Tabelle 0-1: Kombination von Verhaltenskreuz und Normenkreuz

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!

4. Interessenkonflikte

Eine besondere Art von Security-Konflikten sind Interessenkonflikte. Diese treffen vor allem Sicherheitsexperten, die ihre Arbeit nur nebenamtlich machen. Überall wo unterschiedliche Interessen aufeinanderprallen, kann man von Interessenkonflikten sprechen. In diesem Sinne beschäftigt sich das ganze Buch „Konfliktmanagement für Sicherheitsprofis“ mit Interessenkonflikten. Im folgenden 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.

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 dringend bis nächste Woche fertig werden muss*“. Wenn der betroffene Personalbearbeiter jedoch schon am Dienstag zu seinem Abteilungsleiter sagen würde, dass er am Verfahrensverzeichnis nach §4e BDSG arbeiten muss, dann „*hat das sicher auch noch bis Donnerstag Zeit*“.

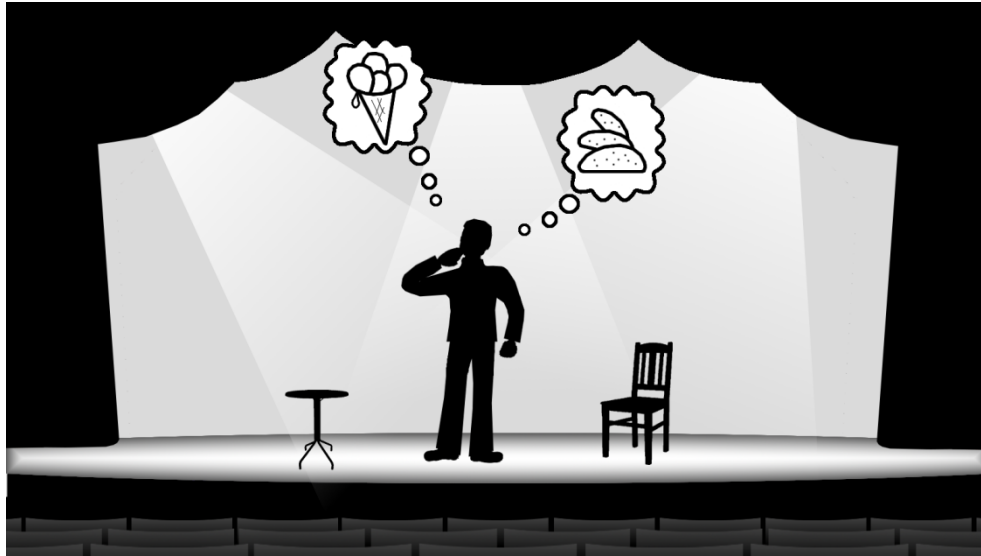


Abbildung 6: Interessenkonflikt: Gemischtes Eis oder lieber trocken Brot

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.“*⁷

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. An dieser Stelle sei auf einen Abschnitt im Buch hingewiesen, der sich gezielt mit den Chancen einer fruchtbaren Zusammenarbeit mit den Personal und Interessenvertretungen beschäftigt.

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) 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!

⁷ BAG; Beschluss des 1. Senats; Mitbestimmung des Betriebsrates bei Versetzung eines Datenschutzbeauftragten; 22.03.1994; Aktenzeichen: 1 ABR 51/93 ↗

Wer kontrolliert den Kontrolleur?

In einem anderen Abschnitt im Buch „Konfliktmanagement für Sicherheitsprofis“ steht 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.⁸

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 zuvor bereits erörtert haben. Insbesondere unterliegen die Betroffenen in dieser Situation in ihrer Haupttätigkeit denselben Zwängen, wie die normalen Mitarbeiter und schnell werden in einer „drive-by“-Risikoanalyse auch dieselben Fehleinschätzungen getroffen.

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.

5. Fallbeispiel: Mehr Unterstützung vom Chef

Bisher haben 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

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

Problemen des Alltags unterscheidet. Zum Abschluss des vorliegenden Auszugs aus dem Buch „Konfliktmanagement für Sicherheitsprofis“ geht der Fokus in die Firma für die Fallbeispiele des Buchs: Die ExAmple AG. Hier arbeiten die Sicherheitsexperten Alice (Datenschutz), Bob (IT-Sicherheitsbeauftragter) und Dave (Werkssicherheit).

In einem der Fallbeispiele sind die drei übereingekommen⁹, 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 bemängelte, dass der Vorstand kaum Interesse an den Vorfällen der letzten Zeit zeigte. Jetzt sitzen sie wieder zusammen und überlegen, wie sie ihr Ziel erreichen können.

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. Nach ein paar Minuten haben sie ihre Ideen auf dem Flipchart zusammengeschrieben:

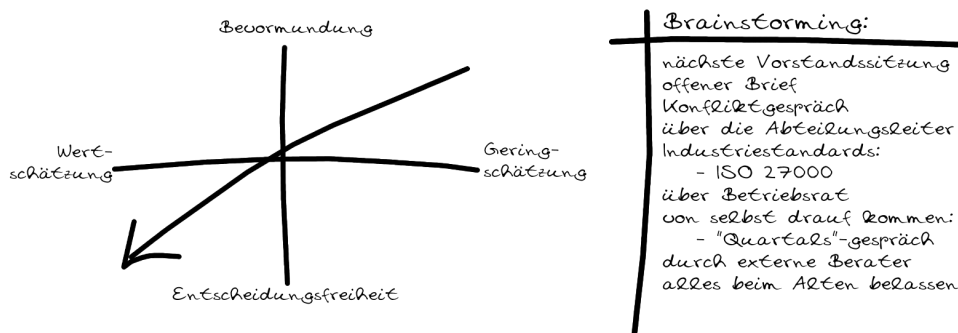


Abbildung 7: Alice, Bob und Dave analysieren ihre Situation

⁹ Dieses Fallbeispiel finden Sie im OnlinePLUS-Service zum Buch im Internet unter <http://www.viewegteubner.de/tu/Konfliktmanagement>

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 *größter 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.

6. 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 dieser Auszug aus dem Buch „Konfliktmanagement für Sicherheitsprofis“ die verschiedenen Arten von Security-Konflikten.

Den ersten 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.

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 sie sich in den weiteren Kapiteln des Buchs einem der Hauptziele: Der Vermeidung von Konflikten.

Informationen zum Bezug des Buchs:

Sie erhalten das Buch „Konfliktmanagement für Sicherheitsprofis“ überall online sowie im regulären Buchhandel oder direkt beim Vieweg+Teubner Verlag.

Weitere Informationen finden Sie unter <http://www.viewegteubner.de/tu/Konfliktmanagement>.