Edition <kes>

Sebastian Klipper

Konfliktmanagement für Sicherheitsprofis

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

3. Auflage

<kes>

Springer Vieweg

Edition <kes>

Mit der allgegenwärtigen IT ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Die <kes> – Zeitschrift für Informations-Sicherheit – wird von der DATAKONTEXT GmbH im zweimonatigen Rhythmus veröffentlicht und behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz. Nähere Informationen rund um die Fachzeitschrift finden Sie unter www.kes.info.

Die Autoren der Zeitschrift und der Buchreihe Edition <kes> helfen den Anwendern in Basic- und Expert-Seminaren bei einer praxisnahen Umsetzung der Informations-Sicherheit: www.itsecuritycircles.de

Weitere Bände in dieser Reihe http://www.springer.com/series/12374

Sebastian Klipper

Konfliktmanagement für Sicherheitsprofis

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

3. Auflage

Springer Vieweg

Sebastian Klipper
Hamburg, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-31840-6 ISBN 978-3-658-31841-3 (eBook)
https://doi.org/10.1007/978-3-658-31841-3

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

Planung: Petra Steinmüller
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Dank

„Begegnet uns jemand, der uns Dank schuldig ist, gleich fällt es uns ein. Wie oft können wir jemandem begegnen, dem wir Dank schuldig sind, ohne daran zu denken!“
-- Johann Wolfgang von Goethe

Ich möchte all meinen Mitarbeitern, Kollegen und Auftraggebern danken, mit denen ich in den vielen Jahren als IT-Sicherheitsbeauftragter und Security Consultant intensiv an neuen Ideen und Sicherheitslösungen arbeiten konnte.

Weiterer Dank gilt den Lesern der ersten beiden Auflagen, die das Buch so erfolgreich gemacht haben. Zehn Jahre nach der ersten Auflage, einem Nachdruck und der zweiten überarbeiteten und ergänzten Auflage 2015 liegt nun auch die dritte überarbeitete Auflage vor.

Vorwort zur ersten Auflage 2010

„Am Anfang wurde das Universum erschaffen.
Das machte einige Leute sehr wütend und
wurde allenthalben als ein Schritt in die
völlig falsche Richtung bezeichnet."
-- Douglas Adams
in „Das Restaurant am Rande des Universums"

Langweiliges Sachbuch?

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."*

Schwerpunkt: Kommunikation

Dieses Buch möchte Sie mit den nötigen Mitteln wappnen, die den Weg durch die Untiefen der Security-Kommunikation weisen. Dabei soll es nicht so verstanden werden, dass nur Kommunikation wichtig wäre und technische Sicherheitsmaßnahmen

nicht erfolgreich sein könnten. Sie sind und bleiben weiter wichtig. Das wäre dann 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.

Risiko Nr. 1

Während sich schon seit Langem Bücher[1] damit befassen, wie man den Faktor Mensch dazu bringt, gegen Sicherheitsregeln zu verstoßen, gibt es nur wenige Bücher[2], die sich das Gegenteil zum Schwerpunkt machen. Dabei besteht meist Einigkeit, 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 nahezu keins darüber, wie man Entscheider dazu bringt, die nötigen Mittel für Sicherheitsmaßnahmen zur Verfügung zu stellen oder wie man die Mitarbeitenden motiviert, keine Wettbewerbe im Umgehen von Sicherheitsmaßnahmen zu veranstalten. Diese Lücke soll mit diesem Buch geschlossen werden.

Leitsätze

Am Ende des Buchs wird einer der zehn 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 voranbringen 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

Vorwort zur zweiten Auflage 2015

„Der Irrtum wiederholt sich immerfort in der Tat. Deswegen muss man das Wahre unermüdlich in Worten wiederholen."
-- Johann Wolfgang von Goethe

Motivation zur Neuauflage

Als ich vor fünf Jahren begann, an der ersten Auflage dieses Buchs zu schreiben, dachte ich noch nicht im Traum daran, dass ich irgendwann eine zweite Auflage bei meinem Verlag vorlegen würde. Glücklicherweise werden Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co. jedoch nach wie vor gebraucht und nach wie vor schlagen sie sich mit den gleichen Problemen herum – genau wie vor fünf, zehn oder 15 Jahren.

Unsere Branche wird von den immer gleichen Irrtümern gestützt, die bei Mitarbeitenden und Führungskräften zu den immer gleichen *„Taten"* führen und es ist unsere Aufgabe, den Schaden, den diese irrigen Taten anrichten, möglichst gering zu

halten und manchmal, aber nur manchmal gelingt es uns vielleicht auch eine solche Tat zu verhindern.

Im Grunde hat sich also an der Situation in den letzten fünf Jahren kaum etwas verändert. Trotz allem ist die Technik vorangeschritten und so kommt manches Detail in der ersten Auflage etwas altbacken daher. Und auch ich als Ihr Autor habe mich weiterentwickelt und neue Erfahrungen gewonnen, die ich gerne in der ein oder anderen Weise mit einfließen lassen möchte.

Edward Snowden

Natürlich komme ich nicht durch dieses Vorwort ohne ein Wort über den Wistleblower Edward Snowden zu verlieren. Im Sommer 2013 begann durch seine Enthüllungen eine bisher nicht dagewesene Auseinandersetzung mit dem Thema Informationssicherheit. Vom *„normalen"* Bürger über Journalisten bis hin zur Bundeskanzlerin und ihrem Handy: In der Post-Snowden-Ära steht fest, dass jeder potentielles Opfer von Spähangriffen ist. Die meisten Sicherheitsprofis indes hat das nicht unvorbereitet getroffen oder gar überrascht. Den meisten war klar, dass es genau so läuft. Auch wenn jetzt in vielen Unternehmen mehr in Sicherheit investiert wird, Geld löst nicht alle Probleme und schon gar nicht die Konflikte, die dabei entstehen, neue Sicherheitsmaßnahmen zu planen und vor Allem umzusetzen. Was das angeht, ist das Problem der Sicherheitsprofis im Grunde größer geworden, da man jetzt vor dem Problem steht, seinem Unternehmen unter Umständen noch mehr *„Change"* angedeihen zu lassen als das in der Vergangenheit der Fall war.

Mehr Praxis, Inputs und Projektbezug

Auch ohne dass die in der ersten Auflage beschriebenen Ideen an sich veraltet sind, gab und gibt es viele neue Erfahrungen und Anekdoten aus der Praxis, die in das Buch eingeflossen sind. Nicht zuletzt sind auch die vielen Ideen und Hinweise eingeflossen, die ich von den bisherigen Lesern und Zuhörern bei meinen Vorträgen zum Buch erhalten habe. Darüber hinaus findet insbesondere das Thema *„Security in Projekten"* überall da stärkere Berücksichtigung, wo die erste Auflage sich im Schwerpunkt auf die Linienfunktionen der Sicherheitsprofis konzentriert hat. Hierzu enthält die zweite Auflage ein eigenes Kapitel, dass sich an die Securityprofis richtet, die in einer Projektorganisation für dieses Thema Verantwortung tragen.

Neues Layout

Nicht zuletzt wurde auch das Layout überarbeitet, um dem Buch ein frischeres Antlitz zu verleihen und die Lesbarkeit zu erhöhen. So erleichtern die hinzugekommenen Randnotizen die Orientierung und liefern das Schlagwort zum vor Ihnen liegenden Abschnitt.

Ich wünsche Ihnen viel Spaß mit der 2. Auflage von „Konfliktmanagement für Sicherheitsprofis“ und viel Erfolg bei der Umsetzung der vorgestellten Konzepte.

Sie werden damit wahrscheinlich nicht immer erfolgreich sein – genauso wenig wie ich, aber Sie werden sicher die ein oder andere Klippe umschiffen, die Ihnen vorher vielleicht den Untergang gebracht hätte.

In diesem Sinne,
Ihr Sebastian Klipper

Vorwort zur dritten Auflage 2020

Es ist unmöglich, einen unnötigen Konflikt zu beginnen.
Ob der Konflikt unnötig war, findet man erst heraus,
wenn er längst in Gange ist.

10 Jahre Security-Konfliktmanagement

Vor zehn Jahren war die Welt der Informations- und IT-Sicherheit nicht die gleiche wie heute. Der Begriff Cybersicherheit spielte in der ersten Auflage dieses Buches überhaupt noch keine Rolle und Cyberkriminelle hatten gerade erst begonnen ein Geschäftsmodell zu entwickeln, dass uns aktuell mit Ransomware, CEO-Fraud und anderen Maschen in Atem hält. Viel hat sich getan in den letzten Jahren.

Die Konstanten

Andere Dinge sind für Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co. aber auch gleichgeblieben. Dazu gehört insbesondere die menschliche Neigung den Überbringer einer schlechten Nachricht für deren Inhalt verantwortlich zu machen. Nach wie vor droht den Informations- und IT-Sicherheitsbeauftragten, Datenschützer,

CISOs und Co. deshalb die Buhmann-Falle. Diese Konstante zeigt sich überdeutlich in dem nachfolgenden Vorwort, dass Prof. Dr. Sebastian Schinzel zur ersten Auflage geschrieben hat und darin von einer Anekdote berichtet, die mittlerweile 20 Jahre zurück liegt. Aus diesem Grund habe ich mich auch gemeinsam mit dem Verlag entschlossen, das Buch für Sie zu überarbeiten und an die aktuelle Situation der Informations- und IT-Sicherheit anzupassen.

Neue Begriffe

Am augenfälligsten sind diese Anpassungen bei den veränderten Begriffen. Hieß es in der ersten Auflage im Untertitel des Buchs noch „Auswege aus der „Buhmann-Falle" für IT-Sicherheitsbeauftragte, Datenschützer und Co." haben wir diese Zeile geändert zu „Auswege aus der „Buhmann-Falle" für Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co." Statt von Informationssicherheit werden wir häufiger von Cybersicherheit sprechen und beim Datenschutz stärker auf den technischen Datenschutz abheben als auf juristische Fragestellungen.

Geschlechtsneutrale Bezeichnungen

Darüber hinaus wurde die 3. Auflage mit weitestgehend geschlechtsneutralen Bezeichnungen überarbeitet. An einigen Stellen wurden männliche und weibliche Formen im losen Wechsel verwendet, wenn es im Kontext passt. Auf Formulierungen wie *‚Datenschützer und Datenschützerinnen'* wurde zugunsten der besseren Lesbarkeit verzichtet. Die verbliebenen grammatikalisch männlichen Bezeichnungen wie z. B. *‚Kunden'*, *‚Angreifer'* oder *‚Täter'* schließen im Plural natürlich immer weibliche, männliche und andere Identitäten ein.

Viel Spaß beim Lesen und
viel Erfolg in den nächsten Jahren,
Ihr Sebastian Klipper

Geleitwort zur ersten Auflage

von Prof. Dr. Sebastian Schinzel, Fachhochschule Münster

Perfekt vorbereitet

Irgendwann vor zehn Jahren hatte ich als Junior-Unternehmensberater meinen ersten Penetrationstest bei einem Unternehmen. Ich sollte ein SAP-System auf Sicherheitslücken untersuchen und das Ergebnis war verheerend. Sicherheitslücken wie Sand am Meer, was darauf schließen ließ, dass die Entwickler keinen blassen Schimmer von sicherer Softwareentwicklung hatten. Die gefundenen Lücken hatte ich penibel dokumentiert und deren Kritikalität konnte ich über real funktionierende Exploits beweisen. Damit bei der Abschlusspräsentation auch nichts schief ging, hatte ich Videoaufzeichnungen meiner Angriffe vorbereitet und die SQL-Datenbank mit den Bewerberdaten (Testdaten), die ich über einen Angriff abgezogen hatte, auf einem USB-Stick in der Tasche stecken. Ich war perfekt vorbereitet.

In der Abschlusspräsentation des Penetrationstests saßen dann einige der beteiligten Entwickler, der Entwicklungsleiter und ein Manager. Ich freute mich auf die Präsentation, schließlich waren die gefunden Schwachstellen hochkritisch und durch meine

Arbeit wurde verhindert, dass dieses System in diesem unsicheren Zustand produktiv gestellt wurde.

„Buhmann-Falle“ schnappt zu

Doch es kam anders. Kaum hatte ich angefangen, wurde ich minütlich vom Entwicklungsleiter unterbrochen. Das wäre ja alles nicht so schlimm und viele der Schwachstellen wären aus irgendwelchen technischen Detailgründen auf dem Produktivsystem vielleicht gar nicht ausnutzbar. Und der Rest der Angriffe würde ja eh in der Firewall „kleben bleiben“, schließlich war die ja teuer und der Firewall-Admin ja sehr kompetent. Um die konkrete Bedrohung abzuschätzen, müsse ich die Angriffe ja alle nochmal gegen das Produktivsystem laufen lassen. Es wäre ja ärgerlich, dass das Budget schon aufgebraucht sei. Nein, eine Aufstockung ist leider nicht möglich. Tja, dann müsse man ja mangels Beweisen davon ausgehen, dass die gefunden Schwachstellen höchstens akademische Relevanz haben und man dann weitgehend unverändert online gehen könne.

Konflikte vergeuden Ressourcen

Was lief hier schief? Offensichtlich hatte der erfahrene Entwicklungsleiter mit einigen rhetorischen Kniffen die Präsentation soweit sabotiert, dass am Ende von den konkret bestehenden Risiken scheinbar nichts mehr übrig war. Es dauerte einige Zeit, bis ich die Motivation dahinter verstand. Das Entwicklerteam hatte monatelang entwickelt, ohne jemals klare Ansagen über die Sicherheitsanforderungen zu bekommen. Selbst wenn es Sicherheitsanforderungen bekommen hätte, hätten die Entwickler wahrscheinlich nicht die Kompetenz gehabt sie umzusetzen, weil sie niemals in sicherer Softwareentwicklung geschult wurden. Sie wurden also am Projektende anhand von Kriterien bewertet, die sie zum einen nicht kannten und zum anderen nicht umsetzen konnten. Das ist unfair und wer sich unfair behandelt fühlt, handelt selber unfair. Dies ist nur eine von den vielen möglichen "Buhmann-Fallen", die man als Informationssicherheitsprofi in Projekten erleben kann. Die daraus entstehenden Konflikte vergeuden wertvolle Ressourcen und behindern Maßnahmen zur Absicherung.

Wie man diese Fallen im Voraus erkennt und vor allem wie man seinen Teil zur Vermeidung beitragen kann, das erklärt Sebastian Klipper in diesem Buch. Als Fundament verwendet er die

relevanten Modelle aus der Psychologie- und der Soziologie-Literatur und bildet diese auf gängige Probleme in Informationssicherheits-Projekten ab. Die Anekdoten aus dem Arbeitsalltag von Sebastian Klipper machen diese Wissensbasis lebendig und das Buch zu einer fesselnden Lektüre, die Sie wahrscheinlich – genauso wie mich – an der ein oder anderen Stelle zum Schmunzeln bringen wird.

Egal ob Sie eine technische, fachliche oder betriebswirtschaftliche Sicht auf die betriebliche Informationssicherheit haben ist: Das Buch sollte zur Standardlektüre von jedem gehören, der konstruktiv zur Informationssicherheit beitragen möchte.

Inhaltsverzeichnis

1. Kapitel

1 Einführung

Sprung ins kalte Wasser

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 2 – Willkommen auf der Security-Bühne auf Seite 7 zu springen. Dort wird eine Szenerie beschrieben, wie sie Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co. jeden Tag erleben können. Für diese und andere Problemsituationen liefert dieses Buch Lösungsmöglichkeiten.

Nur was für Hartgesottene

Was macht die Probleme der Sicherheitsprofis eigentlich so speziell? Wir wollen versuchen, uns der Beantwortung dieser Frage langsam zu nähern: Wenn es keine Sicherheitsvorfälle gibt, will niemand all die Informationssicherheitsbeauftragten, Datenschutzbeauftragten oder Information Security Officers sehen. Sie gelten als Spielverderber, Bedenkenträger und Fortschrittsverhinderer. Viele Sicherheitsprofis 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

S. Klipper, *Konfliktmanagement für Sicherheitsprofis*, Edition <kes>,
https://doi.org/10.1007/978-3-658-31841-3_1

die Schuldige gesucht: *"Warum haben unsere Cyber-Experten nichts dagegen unternommen?"*

Die Welt der Cybersicherheit ist voller Missverständnisse und Konflikte, die ein hohes Maß an Kommunikationsstärke und Konfliktfähigkeit erfordern. Dieser Job ist – machen wir uns nichts vor – nur etwas für Hartgesottene mit Durchhaltevermögen.

Geladen und entsichert

Entweder man wechselt nach wenigen Jahren wieder zurück in den unsicheren Teil der Unternehmenswelt, oder man hält durch und kämpft gegen den immer wiederkehrenden Versuch seiner *„Gegenspieler"* sich und ihr Unternehmen zu *„entsichern"*. Dabei kann der Job durchaus Spaß machen, wenn man sich auf die beteiligten Akteure, ihre Sorgen und Zwänge besser einstellt.

Mausefalle Security

Welcher Sicherheitsprofi kennt das nicht: Sicherheitsmaßnahmen lösen Widerstand aus und sorgen für Konflikte. Sicherheitsprofis leben tagein, tagaus mit Begriffen wie *Bedrohung*, *Risiko* oder *Schwachstelle*. Für die, die die ersten Jahre im Job überstehen, ist die Security-Branche eine Mausefalle. Wer einmal in dieser Falle gefangen ist, findet selten den Ausgang, der zurück in den vormaligen Geisteszustand leitet.[3] In vielen Fällen stand die Tätigkeit im Bereich der Cybersicherheit nicht einmal auf dem Berufswunschzettel.[4]

Denken in Risiken

Sicherheitsprofis denken mit der Zeit in Risiken und nach und nach geht das Wissen darüber verloren, dass man auch ein Leben führen kann, in dem man sich nicht immer und immer wieder die Frage stellt, was bei dieser oder jener Sache alles schief gehen kann. Auch das ist ein Ursprung der vielfältigen Konflikte in der Security-Welt: Und so verlieren wir mit der Zeit das Verständnis für Menschen, die in Chancen denken und nicht in Risiken.

Blick über den Tellerrand

Stöbert man in der Buchhandlung durch das Angebot an Konfliktliteratur, wird man mit einem fast unüberschaubaren Angebot konfrontiert. Eine Vielzahl von Büchern versprechen

---

[3] Frei nach Egmont Colerus, der das Bild zum veränderten Geisteszustand für die Mathematik benutzt; Vom Einmaleins zum Integral; 1947; Zsolnay; ASIN: B0000BH6NV

[4] known_sense (Herausgeber); Aus der Abwehr in den Beichtstuhl – Qualitative Wirkungsanalyse CISO & Co.; 2008; known_sense; Seite 11

Lösungen für die Konflikte des Alltags. Betrachtet man als Sicherheitsprofi dann die 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 man sich im Bereich der Cybersicherheit jeden Tag stellen muss, 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 in den gängigen Jobs der Branche an.

Kapitel 1

In dieser Einführung wird ein grober Überblick über die Motivation für dieses Buch gegeben und Sie erhalten einen groben Überblick über die vor uns liegenden Kapitel.

Kapitel 2

Im zweiten Kapitel über die Security-Bühne werden die Hauptakteure vorgestellt, mit denen die Beauftragten für physische Sicherheit, Informationssicherheit und technischen Datenschutz zu tun haben – allen voran das Top-Management. 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 Mitarbeitenden 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.

Kapitel 3

Nachdem im zweiten Kapitel die Hauptakteure unter die Lupe genommen wurden, befasst sich Kapitel 3 mit der Frage, was Security-Konflikte sind und was sie von anderen Konflikten unterscheidet. Warum geraten gerade Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs 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 Cybersicherheit nur der Zweit- oder gar Dritt-Job ist?

Kapitel 4

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 vierten Kapitels. Wie vermeidet man durch eine klare Kommunikation konsequent die Art von Missverständnissen, die in den ersten Kapiteln betrachtet wurden? Wie motiviert man mit Live-Hackings und Penetration-Tests auch das unmotivierteste Management und welche Bedeutung haben Awareness-Kampagnen für die Motivation der Mitarbeitenden. 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.

Kapitel 5

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 fünfte 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 fünften Kapitels, das Sicherheitsprofis darüber hinaus dazu aufruft: *„Tue Gutes und rede darüber“*.

Kapitel 6

Was aber gibt es für Möglichkeiten, wenn der Widerstand der Mitarbeitenden überhandnimmt und einfach nichts funktionieren will? In solchen Fällen ist es notwendig, den strittigen Sicherheitsmaßnahmen in geregelten Eskalationsstufen Gehör zu verschaffen. Das sechste 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 Mitarbeitende, Top-Management 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.

Kapitel 7

Dieses Kapitel ergänzte bereits die zweite Auflage um die Aspekte des Konfliktmanagements, die sich speziell in Projekten ergeben. Wir betrachten dazu die Unterschiede und Gemeinsamkeiten der Arbeit in Linie und Projekt und stellt zusätzliche Interessengruppen vor, die das Projektgeschäft bestimmen. Die Projektarbeit hält einiges an Herausforderungen für Informations- und IT-Sicherheitsbeauftragte, Datenschützer, CISOs und Co. bereit. In der dritten Auflage werden wir dabei auch auf die Herausforderungen des agilen Projektmanagements unter dem Schlagwort DevSecOps eingehen.

Kapitel 8

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

❖❖❖

Machen Sie sich Notizen

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 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 aus Papier zu kaufen? Nutzen Sie diese Möglichkeiten.

Offene Quellen

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, können zusätzlich im ursprünglichen Zustand, in dem sie gesichtet wurden auf http://www.archive.org nachrecherchiert werden. Archivierungen der ersten Auflage unter http://www.webcitation.org sind leider nicht mehr verfügbar.

2. Kapitel

2 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 dieser Welt-Bühne spielt sich der Alltag von Informations- und IT-Sicherheits-beauftragten, Datenschützern, CISOs und Co. ab.

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

[5] Erving Goffman; Rahmen-Analyse. Ein Versuch über die Organisation von Alltagserfahrungen; 1996; Suhrkamp; ISBN 978-3518279298

S. Klipper, *Konfliktmanagement für Sicherheitsprofis*, Edition <kes>,
https://doi.org/10.1007/978-3-658-31841-3_2