

## Einleitung

*„Wie alles sich zum Ganzen webt,  
Eins in dem andern wirkt und lebt!“*

*(J. W. v. Goethe, Faust I)*

Der Begriff „Sicherheit“ wird allgemein im zivilen beziehungsweise privatwirtschaftlichen Umfeld, insbesondere aber bei Betrachtungen hinsichtlich „IT-Sicherheit“ in der IT, sehr ungenau oder gar nicht definiert. Aus diesem Umstand entsteht, neben vielen bunten und zumeist wertlosen Floskeln aus den Marketing-Abteilungen diverser Unternehmen, eine nicht unbedeutende, weil folgenreiche Ungenauigkeit bei der Verwendung und Interpretation dieses Begriffes.

Während sich die Inhalte des Begriffs „Sicherheit“ in vielen Bereichen des täglichen Lebens bei näherer Betrachtung oft schnell und hinreichend genau beschreiben lassen, gestaltet sich die Situation in der IT wesentlich komplexer. Aufgrund der Komplexität und des allgemein hohen Grades der Vernetzung aktueller IT-Systeme gelangt eine Vielzahl nicht unmittelbar IT-technischer Aspekte in den Wirkungsbereich der IT-Sicherheit. Hinzu kommen die individuellen, jeweils situationsabhängigen Sicherheitsbedürfnisse, die die klare Abgrenzung der Begriffe weiter erschweren; denn je nach individuellem Aufgabengebiet erkennt der eine spezifische Bedürfnisse, die einem anderen in dieser Ausprägung nicht auffallen würden und vice versa. Unter anderem deswegen hat sich die „IT-Sicherheit“ mittlerweile als klassische Querschnittsdisziplin mit Prozesscharakter etabliert. Ähnlich wie in klassischen sicherheitssensitiven Umfeldern wie z.B. militärischer Informationsverarbeitung findet auch im privatwirtschaftlichen Umfeld einhergehend mit dem Bewusstseinswandel eine Transformation der IT-Sicherheit hin zum wirtschaftlich und auch funktional essentiellen „Enabling Factor“ statt. Eine starke Affinität der IT-Sicherheit mit den ebenfalls querschnittlichen Themen im Bereich „Regulatory Compliance“ verstärkt die Transformation und gibt dem Anteil der technischen Realisierung Auftrieb.

Einen interessanten Aspekt in der historischen Betrachtung jener Entwicklung – welche sicherlich noch nicht abgeschlossen ist – stellt z.B. die offensichtliche Korrelation mit der Entwicklung des Systems Management dezentraler Client/Server-Systeme vor einigen Jahren dar. Dies lässt sich sowohl auf die eher technischen Aspekte wie z.B. Spektrum und Reifegrad verfügbarer Tools

sowie deren Implementierungen beziehen als auch auf die wachsende Komplexität und eher organisatorischen Aspekte wie z.B. die evolutionäre Entwicklung von Standards und „Best Practices“.

Dieser Vielschichtigkeit und Komplexität muss und will natürlich auch dieses Buch Rechnung tragen. Wir versuchen das, indem wir zunächst die aus den oft verwirrenden Zusammenhängen der technisch relevanten Themen entstehende Komplexität auf ein Mindestmaß reduzieren und so einen Überblick des Ganzen zu vermitteln suchen. Denn allzu häufig fällt auch sonst fachkundigen Interessierten bereits der Einstieg in die Thematik schwer, und das bei sowieso ansehnlichem Frustrationspotential der Gesamthematik in Anbetracht der multidimensionalen Komplexität. Sicherlich ist es aber auch genau diese Komplexität, dieser stetige Fortschritt in Technologie und deren Anwendung beziehungsweise Missbrauchspotential und die somit messbar steigende Relevanz in der realen Welt, die eine Beschäftigung mit dem Thema „IT-Sicherheit“ fachlich herausfordernd und wirtschaftlich gleichsam lohnenswert wie auch notwendig erscheinen lässt.

## 1.1 Für wen dieses Buch interessant ist

So oft wir auch in Buchhandlungen, Büchereien, im Internet oder auf Veranstaltungen und Treffen unterwegs waren, wir haben bis heute noch kein Buch und keine zusammenhängende Dokumentation zum Themengebiet „IT-Sicherheit“ gefunden, das sich auf konzeptionell übergreifender Ebene an uns richtet. Die Wahrscheinlichkeit, dass sich dieser Umstand bis zum Erscheinen dieses Buches geändert hat, schätzen wir als gering ein.

Wir richten uns mit unserem Buch in erster Linie an Fachleute und solche, die es werden wollen. Es ist für Menschen aus anderen Fachrichtungen der IT, die sich in das Thema einarbeiten wollen ebenso gedacht wie für fachlich vorgebildete Menschen, um jene bei der Auseinandersetzung mit der Materie zu unterstützen.

## 1.2 Warum dieses Buch entstand

In Rahmen unserer Tätigkeit als Berater kamen und kommen wir immer wieder mit sicherheits- sowie IT-sicherheitsrelevanten Fragen in Berührung, meist bedingt oder auch tangiert von Aspekten des Datenschutzes, der Prozessoptimierung oder auch Wettbewerbsfähigkeit. Sei es nun im Zusammenhang mit entsprechenden Projekten oder, quasi als Nebenprodukt, aus an sich nicht unmittelbar zum Thema „IT-Sicherheit“ zuzuordnenden Einsätzen. Klassischen „Enabling Factors“ und Querschnittsdisziplinen entkommt man nicht so ohne weiteres.

Das Thema „IT-Sicherheit“ geistert quer durch alle Bereiche, es berührt jeden Bereich der Technik und jedes Aufgabengebiet der Anwender – aber ein

echtes Sicherheitsbewusstsein haben wir nur in den seltensten Fällen erleben können. Interessanterweise lässt sich hier leider feststellen, daß die im klassischen Sinne sicherheitsbewussten Bereiche im behördlichen oder militärischen Umfeld genauso wie kritische Infrastrukturen im zivilen Umfeld und auch von IT nahezu 100-prozentig abhängige Organisationen wie z.B. Banken oder Versicherungen bei der operativen Umsetzung von IT-Sicherheit trotz verstärktem institutionellem Fokus durchaus viel Optimierungspotential bei Umsetzung und Beachtung von Maßnahmen zur IT-Sicherheit aufweisen. Je-ner Zustand legt den Rückschluss sowohl auf mangelndes Sicherheitsbewusstsein als auch auf teilweise eher gewissensberuhigenden Maßnahmenfokus nahe. „Zu kompliziert“ werden die Techniker gerne kolportiert, „zu teuer“ ächzt vielerorts das Management und den Anwendern wird gar nachgesagt, sie würden aus Starrsinn und Bequemlichkeit einmal eingeführte Sicherheitsmaßnahmen konsequent unterlaufen.

Aber ist es denn wirklich immer so? Sind die angeordneten Maßnahmen wirklich zu kompliziert in Implementierung und Handhabung? Werden die Bedürfnisse und Fähigkeiten der Anwender tatsächlich immer und immer wieder ignoriert? Wir glauben, dass dies wohl allzu häufig stimmt, Einschränkungen in Funktion und Handhabung allerdings nur wirklich selten zwingend notwendig sind. Es muss nicht immer umständlich und kompliziert zugehen, wenn Sicherheit zielgerichtet ein- und umgesetzt werden soll, und doch scheint einerseits die Hemmschwelle zur Einrichtung konsistenter Vorgaben und Maßstäbe erstaunlich hoch und andererseits die Akzeptanz für derartige Maßnahmen und deren Auswirkungen erstaunlich niedrig zu sein. Sicherlich eine – durch viele Erfahrung validierte – Binsenweisheit ist, dass nachträgliches „Aufzwingen“ der IT-Sicherheit, Nacharbeiten unter Zeit- und Ergebnisdruck und Änderungen oder Einschränkungen an Systemen stets für alle Beteiligten mehr Reibungsverluste und Kosten mit sich bringt als eine proaktive Betrachtung auf funktional wie auch wirtschaftlich angemessener Grundlage und pragmatischer Verhältnismäßigkeit von Anfang an.

Zumindest auf Seiten der administrativ und technisch Verantwortlichen beziehungsweise Einflussnehmer hoffen wir, diese Problematik durch die Vermittlung eines übergreifenden Grundwissens entschärfen zu können. Auch wenn dieses Buch dem unbedarften Anwender oder versierten Fachmann uninteressant erscheinen mag – für die breite Gruppe der interessierten und fachlich zumindest grundlegend vorgebildeten Anwender, Administratoren und Entscheidungsträger wollen wir ein umfassendes Werk bereitstellen, welches als übergreifende Klammer eine Vielzahl von Fragen beantworten hilft und „nebenher“ vielleicht auch noch mit einigen Vorurteilen aufräumen kann.

## 1.3 Was dieses Buch leistet

Unsere Zielsetzung ist klar und einfach: Nach der intensiven Lektüre dieses Buches soll der Leser in der Lage sein, aufgrund des ihm vermittelten Wissens

und der Erfahrungen auch komplexere Sachverhalte und Zusammenhänge im Themengebiet „IT-Sicherheit“ schnell und sicher zu verstehen beziehungsweise sich diese erarbeiten zu können.

Uns liegt die Vermittlung fundierter Kenntnisse der zugrunde liegenden Technologien, Mechanismen und Zusammenhänge am Herzen. Denn sehr gerne, leider allzu gerne, wird die Erarbeitung und Umsetzung einer konsistenten IT-Sicherheitspolitik mit der wahlfreien Aneinanderreihung beliebiger anwendungs- und Technologiekomponenten verwechselt.

Wir können uns diese Verwechslungen eigentlich nur mit mangelnder Kenntnis der tieferen Zusammenhänge erklären. Diese Annahme ist in keiner Weise negativ bewertet, denn sieht man sich auf dem Buchmarkt um, wird man sehr schnell feststellen müssen, dass es zu fast jedem Spezialgebiet und zu vielen, insbesondere den verbreiteten Anwendungen mindestens ein gutes oder sehr gutes Fachbuch gibt. Kenntnisse der zugrunde liegenden Konzepte, Technologien und Implementationen scheinen hingegen von einer derart ausgeprägten Selbstverständlichkeit zu sein, dass sich hierzu keine wirklich verwendbare Fachliteratur finden lässt. Mit diesem Buch wollen wir aktiv und praktisch dazu beitragen, diesen Missstand zu beheben.

Allerdings erzwingt die immense Komplexität des Themas „IT-Sicherheit“ auch Einschränkungen. Wollten wir versuchen, alle tatsächlich relevanten Themen und Nebenthemen grundlegend zu behandeln, würde die Fertigstellung dieses Buches derartig viel Zeit beanspruchen, dass bereits vor seiner Fertigstellung etliche, vor allem technische Themen wieder veraltet wären und ihre Besprechungen grundlegend überarbeitet werden müssten. Dazu kommt, dass auch Themen, die im Allgemeinen nicht der IT zugeordnet werden, sinnvollerweise dem Themenkomplex „IT-Sicherheit“ zugerechnet werden müssten. Als Beispiel sei hier die Schließtechnik im Kontext der Absicherung eines physischen Systemzugangs genannt. Auch Themen aus der Architektur, Statik und dergleichen spielen unter Umständen gewichtige Rollen.

Unser Konzept beschränkt sich deshalb auf die Technik in der IT. Nicht technische, Rand- und Spezialthemen, lassen wir zur Verringerung der Komplexität außen vor. Einige Spezialthemen die erfahrungsgemäß durchaus, wenn auch eher selten, im Arbeitsalltag eines Administrators auftauchen können, behandeln wir zusammenfassend oder im Rahmen gezielter Exkurse. Dazu gehören unter anderem Themen wie bauliche Maßnahmen (Raum- und Gebäudekonzeption, bauliche Maßnahmen zur Zugangskontrolle, zur Verfügbarkeit, bauliche Infrastrukturmaßnahmen und dergleichen), spezielle Anwendungssoftware und Ähnliches.

Wir setzen zudem voraus, dass grundlegende Kenntnisse der relevanten Konzepte zu System- und Netzwerktechnologien sowie deren Umsetzung bereits vorhanden sind. Das bedeutet nicht, dass umfassende Kenntnisse sämtlicher Technologien vorhanden sein müssen, eine solide Grundlage (engl. *working knowledge*) wäre von Nutzen. Was nicht vom Leser erwartet wird, sind profunde Kenntnisse in der Konfiguration und Anwendung der diversen, auf dem Markt erhältlichen Spezialanwendungen. Auch wenn wir zwangsläufig

einige dieser Werkzeuge für die Beispiele unseres Buches verwenden – wir erläutern die Auswirkungen der im Beispiel getroffenen Maßnahmen und verweisen zudem auf entsprechende Literatur, so dass jedem interessierten Leser Ansatzpunkte für eine Vertiefung des Themas gegeben werden.

## 1.4 Was dieses Buch nicht bietet

Dieses Buch ist kein Allheilmittel. Es bietet weder jederzeit anwendbare und immer funktionsfähige, fertige Lösungen noch simplifizierte „Kochrezepte“.

Entsprechend ist auch davon auszugehen, dass die unkritische Übernahme unserer technischen Beispiele unter Umständen nicht zum gewünschten Effekt, sondern zu gravierenden Schwierigkeiten im Produktionsumfeld führen kann, da dort für uns weder vorhersagbare noch einsehbare Rahmenbedingungen herrschen, denen wir zwangsläufig nicht gerecht werden können. Wir führen in diesem Buch die zugrunde liegenden technischen Konzepte zusammen und versuchen anhand der dadurch geschaffenen Übersicht, dem Leser genügend Rüstzeug an die Hand zu geben, dass er darauf aufbauend eigenständig tragfähige Lösungen erarbeiten und umsetzen kann. Der Einfluss lokaler Rahmenbedingungen, Vorgaben und Anforderungen auf die Erarbeitung und Umsetzung einer „Sicherheits-Infrastruktur“ ist so gravierend, dass ohne diese Kenntnisse eigentlich jeder Ansatz einer konkreten Implementierung von vornherein zum Scheitern verurteilt ist. Nur wer in Kenntnis und unter Berücksichtigung dieser Vorgaben und Anforderungen handelt, hat reale Aussichten auf Erfolg.

Als Ersatz für die Lektüre der einschlägigen Standards und RFCs ist dieses Buch ebenfalls völlig ungeeignet, Gleiches gilt für Spezialthemen. Beides, die Vermittlung allgemeinen Grundlagenwissens und die Darstellung spezieller, über eine allgemeine Relevanz hinausgehender Inhalte, sind weder Bestandteil noch Aufgabe dieses Buches. Genauso, wie wir ein brauchbares allgemeines Grundlagenwissen voraussetzen, erwarten wir von unseren Lesern auch die Bereitschaft, sich nötigenfalls selber in Spezialthemen einzuarbeiten. Unser Ziel ist die zusammenführende Darstellung der sicherheitsrelevanten Grundkonzepte und nicht die Erläuterung von Einzelaspekten. Verweise auf Literatur zu eventuell interessanten oder wichtigen Spezialthemen werden von uns wann immer möglich angegeben.

Wer nach spezifischen Informationen zu einer speziellen Anwendung sucht, wird in diesem Buch nicht fündig werden. Gleiches gilt für eingehendere Besprechungen oder Erläuterungen spezieller Technologien wie etwa Verschlüsselungsalgorithmen und dergleichen. Für derart spezielle Interessen gibt es genügend hochwertige Literatur.

## 1.5 Wie dieses Buch gelesen werden sollte

Dieses Buch ist kein Nachschlagewerk, es sollte vollständig vom ersten bis zum letzten Kapitel gelesen werden. Allerdings haben wir sicherlich auch Themen

behandelt, die für einige Leser momentan nicht relevant sind. Für solche Fälle haben wir die Teile IV, V, VI und VII so gestaltet, dass ein Überspringen einzelner Kapitel den Lesefluss nicht wesentlich beeinträchtigen sollte.

## 1.6 Konventionen im Buch

An dieser Stelle wollen wir den Leser nicht mit der Beschreibung der – eigentlich in nahezu allen Fachbüchern vergleichbaren – Typographie- und Layoutkonventionen ermüden. Das vorliegende Buch entspricht in derlei Konventionen weitestgehend den aus der Fachliteratur bekannten und diese sollten recht intuitiv nachvollziehbar sein. Über qualifizierte Rückmeldungen aller Art mit konstruktivem Inhalt freuen sich die Autoren immer.

## 1.7 Randgedanken

Wir beschäftigen uns in diesem Buch fast ausschließlich mit dem Thema „IT-Sicherheit“ aus der Sicht des Betreibers beziehungsweise Anbieters von IT-Diensten. Wenig Berücksichtigung finden jedoch, auch in der aktuell stattfindenden öffentlichen Diskussion, die Bedürfnisse und Interessen der Anwender und Benutzer von IT-Systemen.

Was hierzulande mit dem Schlagwort „Datenschutz“ zusammengefasst wird, beinhaltet tatsächlich mit Blick auf die technische Umsetzung eine große Bandbreite an Themen und Aspekten der IT-Sicherheit oder mit Bezug darauf.

Die Frage nach den Rechten und Pflichten im Umgang mit persönlichen oder personenbezogenen Daten ist durch die Ereignisse am 11. September 2001 stark in Bewegung geraten. Momentan überwiegt die Ansicht, dass persönliche Rechte hinter die Interessen einer „Allgemeinheit“ zurückzutreten hätten – allerdings hat noch niemand eben diese Allgemeinheit zu ihren diesbezüglichen Ansichten befragt.

Aber auch die in vielen Ländern übliche Praxis nicht offensichtlicher Datenerhebungen lässt Fragen offen. Ist es in Ordnung, dass beliebige Unternehmen willkürlich (und manchmal ist dies sogar der einzige Unternehmenszweck) Bewegungsdaten erheben, speichern und auswerten? Ist es erwünscht, dass vergleichbare Praktiken auch im Einzelhandel betrieben werden, wenn dort auch ab und an die eigentliche Datenerfassung manuell durch entsprechendes Personal erfolgt? Auch ist es fragwürdig, inwieweit beispielsweise Handelsketten durch den Einsatz neuer Technologien wie etwa RFID lediglich die Interessen der Verbraucher im Blick haben – ist die automatisierte, massenhafte Erfassung von Bewegungsdaten in (und möglicherweise auch außerhalb?) den Verkaufsräumen vielleicht mehr als nur ein willkommenes „Abfallprodukt“?

Die Unternehmen, die derartige Methoden verwenden, entwickeln oder selber vertreiben, berufen sich fast ausschließlich auf die durch den Einsatz dieser Methoden und Technologien in den verschiedenen Logistikprozessen mögliche Kostensenkung, die letzten Endes dem Verbraucher in Form niedrigerer Preise zugute käme.

Ist diese Argumentation zulässig? Stimmt die Relation von Nutzen und Risiken, insbesondere Missbrauchsrisiken? Dies sind sicherlich Fragen, auf die sich keine allgemein gültige, geschweige denn allumfassende Antwort finden lässt. Vielmehr erfordern derartige Situationen eine genaue Abwägung von Einzelinteressen, Nutzen und Risiken gegeneinander, und dies individuell durch jeden Betroffenen selbst.

Dennoch ist zu beobachten, dass die Diskussion derartiger Themen in der Öffentlichkeit in den vergangenen Jahren durch die aktuellen Geschehnisse rund um den Terror in der Welt mehr und mehr in den Hintergrund des allgemeinen Bewusstseins gedrängt wurde, was nicht nur zu bedauern ist, sondern vielleicht sogar Anlass zu ernster Sorge bietet.





**Einführung in das Thema „IT-Sicherheit“**



Security@Work

Pragmatische Konzeption und Implementierung von  
IT-Sicherheit mit Lösungsbeispielen auf  
Open-Source-Basis

Eschweiler, J.; Atencio Psille, D.E.

2006, XIV, 334 S., Hardcover

ISBN: 978-3-540-22028-2