

Vorwort

Als ich im Februar vor 10 Jahren mein erstes Buch zum Thema Cloud Computing herausgegeben habe, führte dieses Segment noch ein Nischendasein. Heute gilt Cloud Computing als Motor der Digitalisierung. Neue Geschäftsmodelle werden durch Cloud-Lösungen erst möglich, mobile Zugriffe auf IT-Ressourcen vereinfacht und eine schnellere Skalierbarkeit der IT-Leistungen erreicht. Cloud Computing wird von den meisten Unternehmen in Anspruch genommen und durch die Pandemie nochmal befeuert. Der Trend geht in Richtung Hybrid und Multi Cloud, um die Vorteile unterschiedlicher Provider und Lösungen für das Unternehmen optimal nutzen zu können.

Auch wenn laut einer repräsentativen Studie des Bitkom Public-Cloud-Lösungen weniger anfällig sind für Sicherheitsvorfälle als die eigene IT im Unternehmen¹, häufen sich mit der zunehmenden Nutzung von Cloud Computing Cyberangriffe. Und auch andere Faktoren stellen ein Sicherheitsrisiko für das Cloud Computing dar – angefangen von technischen Störungen über Fehlkonfigurationen, Datenverlust, mangelnde Awareness der Mitarbeiter bis hin zu Compliance-Verletzungen.

Die Verantwortung für die Sicherheit schultern sowohl die Cloud-Nutzer als auch die Cloud-Anbieter. Als grobe Richtlinie gilt das Prinzip: Der Kunde trägt die Verantwortung für „Security in the Cloud“ und der Cloud-Anbieter für „Security of the Cloud“. Es ist im Sinne beider Parteien, gemeinsam die Sicherheit zu verbessern, um jedwede Folgeschäden abzuwenden.

Durch die Cloud-Nutzung verändert sich die Bedrohungslage, und traditionelle Sicherheitskonzepte und -lösungen wie klassische Anti-Malware-Technologien oder Firewalls lassen sich nicht kurzerhand auf das Cloud-Umfeld übertragen bzw. bieten nicht mehr ausreichenden Schutz. Cloud-Sicherheit erfordert neue Konzepte und hochentwickelte Technologien.

¹ Studie: Cloud-Monitor 2020, S. 26, Bitkom Research im Auftrag von KPMG

Das sind die Themen des Buches:

- Technologischer und organisatorischer Wandel durch Cloud Computing
- Veränderte Bedrohungslage durch Cloud-Nutzung
- Verantwortlichkeiten in der Cloud-Nutzung – das Shared-Responsibility-Modell
- Vorgehensweise zur Cloud-Migration unter sicherheitsrelevanten Aspekten
- Vorgehensmodelle und Umsetzungskonzepte für sichere Hybrid, Public und Multi Clouds
- Sicherheitskonzepte und -maßnahmen der Cloud-Anbieter
- Datenschutz und DSGVO-konforme Datenverschlüsselung
- Umsetzung von Zero-Trust-Architekturen
- Kritische Infrastrukturen: Grundlagen, Anforderungen und sicherheitsrelevante Umsetzungskonzepte
- Best Practices zur automatischen Identifizierung und Behebung von Sicherheitslücken in AWS und in Microsoft Azure

Branchen- und anwendungsbezogene Beispiele aus der Praxis runden das Buch ab.

Das Buch richtet sich an Cloud-Nutzer, die sich auf strategischer, organisatorischer und operationaler Ebene mit den Themen Cloud Computing und IT-Sicherheit auseinandersetzen, aber auch an IT-Dienstleister und Berater sowie Studierende und Dozenten, die Kenntnisse im Umfeld von Cloud Computing erwerben oder vermitteln wollen.

Zwölf hochkarätige Autoren konnten dazu gewonnen werden, sich mit Beiträgen am Gelingen des Buches zu beteiligen. Ihnen gilt mein Dank.

Christiana Köhler-Schute

Berlin, im Mai 2021

Inhaltsverzeichnis

Vorwort	5
Management Abstract	13
Herausforderung Cloud Security: Wandel in Technologie und Organisation.....	16
Tino Hirschmann und Marcel Reviol	
1 Wandel der IT	16
1.1 Historie	16
1.2 Cloud.....	21
2 Wege in die Cloud	25
2.1 Vorgehensmodelle für die Cloud-Migration	25
3 Wandel der IT-Organisation	28
3.1 Veränderte Verantwortlichkeiten.....	28
3.2 Veränderte Governance durch Cloud-Nutzung	29
3.3 Übersicht zum Ansatz mit „Security by Design“	31
3.4 Sicherheit in agilen Entwicklungsprozessen.....	32
4 Veränderte Bedrohungslage durch Cloud-Nutzung	33
4.1 Exponierte Lage.....	33
4.2 Cloud-Technologie und Governance	35
4.3 Vertrauen in den Cloud Provider	36
Der integrierte Ansatz bei der Migration in die Cloud: Security by Default	38
Christian Lechner und Andreas Schindler	
1 Einführung	38
2 Hacks and Attacks: Cloud versus On-Premises	38
3 Gefahren abwehren: Wir gehen in die Cloud!?	39
4 Trotz Maßnahmen und geteilter Verantwortung – können Unternehmen Cloud-Services trauen?	39
5 Umfassende Sicherheitsanalyse im Vorfeld klärt Handlungsbedarfe	40
6 Conditional Access – nur ein Aspekt für den Schutz von Daten	41
7 Migration in die Cloud am Beispiel eines Unternehmens aus dem Maschinenbau	42
8 Fazit.....	43

Sicher in die Cloud 44

Ralf Stadler

- 1 Neue Security-Herausforderungen durch die Cloud und wie sie sich erfolgreich meistern lassen 44
 - 1.1 Sicherheitsverantwortung in der Cloud 45
 - 1.2 Auflösung des klassischen Perimeters 46
 - 1.3 Unabhängige Sicherheitsnachweise 46
 - 1.4 Gefahr für die Cloud aus dem Internet der Dinge 47
 - 1.5 Dienstleistungen für ein Cloud-gerechtes 360-Grad-Security-Konzept 48
- 2 Warum Digitalisierungsprojekte einen umfassenden Security-Ansatz erfordern 49
 - 2.1 Flexible Arbeitsmodelle: Perimeter löst sich auf 50
 - 2.2 Hohe Sicherheit durch Zwei- und Multi-Faktor-Authentifizierung 51
 - 2.3 Noch komfortabler mit Token 52
 - 2.4 Risikobasierte Authentifizierung 53
- 3 Offene Hybrid Multi Cloud 54
 - 3.1 Chancen und Risiken in Multi Clouds 54
 - 3.2 Multi-Cloud-Netzwerke absichern 55
 - 3.3 Security eingebaut: die IBM-Cloud 55
 - 3.4 Flexible Erweiterungen für die Cloud: IBM Cloud Paks 56
 - 3.5 Noch mehr Sicherheit in hybriden Multi Clouds: IBM Cloud Paks for Security 57
- 4 Arbeiten in der Cloud 59
 - 4.1 Mittelstand besonders im Fokus 59
 - 4.2 Komplettschutz inklusive: Microsoft 365 60
 - 4.3 Effektiver Cloud-Betrieb 63

**Anwendungsbereitstellung über die oneclick™ Cloud-Plattform:
Ein schlagkräftiges Mittel gegen Cyberkriminalität 64**

Dominik Birgelen

- 1 Einführung 64
- 2 Ziele von Cyberkriminellen und stark ansteigende Bedrohungslage 64
- 3 Zero Trust: Traue niemandem außerhalb und innerhalb des Netzwerks 65
- 4 oneclick™ Plattform vereinfacht die Anwendungsbereitstellung und bietet ein Höchstmaß an IT-Sicherheit 66
- 5 So sicher, dass es bei der Anwendungsbereitstellung über oneclick™ eine integrierte Cyber Assurance ohne Fallprüfung gibt 67

Zero Trust ist eine Reise 69

Michael Doujak und Aarno Aukio

- 1 Sicherheitsrisiken in einer immer digitaleren Welt 69
 - 1.1 Weiterentwicklung der Geräte 69
 - 1.2 Weiterentwicklung der Anwendungen 69
 - 1.3 Von der Perimetersicherheit zu Zero Trust..... 70
 - 1.4 Containerisierung und SaaS..... 70
 - 1.5 DevOps 71
 - 1.6 Angriffe sind die neue Normalität..... 71
- 2 Digitalisierung der Informationssicherheit 72
 - 2.1 Die Grundlagen von Zero Trust 72
 - 2.2 Blaupause für eine Zero-Trust-Architektur..... 72
 - 2.3 Sicherheitsvorteile von Zero Trust 73
 - 2.4 Betriebliche Vorteile von Zero Trust 73
- 3 Grenzen von Zero Trust 74
 - 3.1 Identitäts- und Zugriffsverwaltung als zentraler Service..... 75
 - 3.2 Trennen Sie sich nicht vom zentralen Gateway 75
- 4 Zero Trust ist eine Reise 76
- 5 Schlussfolgerung 77

Datenschutzkonforme Cloud-Nutzung – Best Practices für alle Unternehmensgrößen..... 78

Elmar Eperiesi-Beck

- 1 Paradigmenwechsel: vom Systemschutz zum Datenschutz..... 78
- 2 Formale Betrachtung der aktuellen Gefahrenlage 79
- 3 Sicherheitsmaßnahmen der Cloud-Anbieter 84
- 4 Anwendungen in der Praxis 91
 - 4.1 Sicherheit für Microsoft 365 91
 - 4.2 IoT-Sicherheit..... 92
 - 4.3 Privacy Preserving Analytics 93
 - 4.4 Schnittstellenschutz 94
- 5 Fazit..... 95

Herausforderungen für Kritische Infrastrukturen (KRITIS) 97

Dr. Simon Woldeab

- 1 Welche Regularien sind zu berücksichtigen?..... 97
 - 1.1 Einführung..... 97
 - 1.2 IT-Sicherheitsgesetz 97
 - 1.3 KRITIS-V 99
 - 1.4 NIS-Richtlinie 99

2	Wer ist betroffen?	100
2.1	Kritische Infrastruktur-Sektoren	100
2.2	Schwellenwerte	101
3	Welche Anforderungen sind umzusetzen?.....	104
3.1	Einleitung	104
3.2	Anforderungskatalog für KRITIS (C5).....	105
3.3	Branchenspezifische Anforderungen	105
4	Wie sieht ein Umsetzungskonzept aus?	107
4.1	Einleitung	107
4.2	Einsatz integriertes ISMS.....	108
4.3	Anwendungsfall: Einsatz ISMS für ein Klinikum	109
IT-Sicherheit im klinischen Umfeld.....		116
Prof. Dr. Heiko Meyer		
1	Einleitung.....	116
2	Anforderungen an IT-Systeme in der Gesundheitswirtschaft	117
2.1	Begriffsdefinition Gesundheitswirtschaft	117
2.2	Aspekte zur IT-Sicherheit in der Gesundheitswirtschaft...	118
2.3	Gesetzliche Vorgaben in der Gesundheitswirtschaft.....	120
3	Angriffsarten	124
3.1	Malware.....	125
3.2	Data Leaks	126
3.3	Passwörter	127
3.4	Vernetzte Medizintechnikprodukte.....	128
4	Softwareanwendungen in der Gesundheitswirtschaft	129
4.1	On-Premises-Lösungen	129
4.2	Cloud-Lösungen.....	130
4.3	Hybrid-Cloud-Lösungen	131
5	IT-Sicherheit in der Cloud.....	132
5.1	HIPAA-Compliance	133
5.2	Sichere Datenübertragung	133
5.3	Pseudonymisierung von Daten	134
5.4	Authentisierung	135
6	Zusammenfassung.....	136
6.1	Verbesserung der IT-Sicherheit durch Cloud-Lösungen ..	136
6.2	Mehrwert für die Patienten	136
6.3	Betriebswirtschaftliche Aspekte	137
7	Chancen für die Medizin.....	137

**Best Practices zur automatischen Identifizierung und Behebung
der häufigsten kritischen Sicherheitslücken in AWS 140**

Valeri Milke

1	Vorwort und Aufbau der Best Practices	140
1.1	Sicherheitsbezogene AWS-Services	141
1.2	Relevanteste AWS-Services	142
1.3	Shared Responsibility Model	143
2	Best-Practice-Maßnahmen	144
2.1	Best Practises – architektonische Aspekte	144
2.2	Best Practises – sicherheitsbezogene AWS-Services	146
2.3	Best Practices für die am häufigsten eingesetzten AWS-Services	151
3	Tool-Set zur automatischen Identifizierung und Behebung	156
3.1	Open Source	156
3.2	Kommerziell	156

**Best Practices zur automatischen Identifizierung und Behebung
der häufigsten kritischen Sicherheitslücken in Microsoft Azure 158**

Valeri Milke

1	Vorwort	158
1.1	Shared Responsibility Model	159
1.2	Sicherheitsbezogene Azure-Services	160
1.3	Relevante Azure-Services	161
2	Best-Practices-Maßnahmen	161
2.1	Best Practices – architektonische Aspekte	161
2.2	Best Practises – sicherheitsbezogene Azure-Services	165
2.3	Best Practices für die relevantesten Azure-Services	170
3	Tool-Set zur automatischen Identifizierung und Behebung	174
3.1	Open Source	174
4	Fazit	174

Unternehmensdarstellungen 176

Autorenporträts 185

Abbildungsverzeichnis:

Abbildung 1: Verantwortungsschnitt IT-Security im Shared Responsibility Model	23
Abbildung 2: Leitfäden zur Verbesserung der IT-Sicherheit	47
Abbildung 3: Bausteine eines IT-Security-Betriebskonzeptes	49
Abbildung 4: Funktionen für einen sicheren Zugriff	52
Abbildung 5: IBM Cloud Pak For Security Architecture.....	58
Abbildung 6: Die auf vier Säulen basierende Sicherheitstrategie von Microsoft	61
Abbildung 7: Zero-Trust-Komponenten im Cloud-Umfeld	66
Abbildung 8: Zero-Trust-Architektur	72
Abbildung 9: Das Shared-Responsibility-Modell nach Microsoft.....	85
Abbildung 10: KRITIS-Sektoren und Anlagenkategorien	101
Abbildung 11: Tool-gestützte Umsetzung Klinik-Infrastruktur, fuentis Suite	111
Abbildung 12: Tool-gestützte Umsetzung B3S-Katalog Gesundheitsversorgung, fuentis Suite	112
Abbildung 13: AWS Shared Responsibility Model	143
Abbildung 14: Shared Responsibility Model in the cloud	159
Abbildung 15: Architektur der Remotedesktop-Dienste	163

Tabellen:

Tabelle 1: 4-Stufen-Vorgehensmodell Cloud-Migration mit Sicherheitsmerkmalen	27
Tabelle 2: Bemessungskriterien und Schwellenwerte der Anlagenkategorien	104

Management Abstract

Tino Hirschmann und **Marcel Reviol**, Deutsche Telekom Security, nehmen in ihrem einleitenden Beitrag **Herausforderung Cloud Security: Wandel in Technologie und Organisation** den Leser auf eine kurze Zeitreise mit, um insbesondere jüngeren Lesern den Wandel der IT zu verdeutlichen. Sie geben einleitend einen Überblick über Cloud-Services und -Modelle, erläutern das Shared-Responsibility-Modell und beschreiben vier grundsätzliche Vorgehensmodelle zu Anwendungsmigration in die Cloud. Sie stellen auf der Basis von Security by Design sieben Grundregeln auf, die dazu beitragen, die Angriffsfläche von Attacken zu minimieren. Zum Schluss diskutieren sie sicherheitsrelevante Maßnahmen als Reaktion auf eine veränderte Bedrohungslage durch die Cloud-Nutzung und lassen ihre Erfahrungen einfließen.

Die Frage, ob Unternehmen Cloud-Services trauen können, beantworten **Christian Lechner** und **Andreas Schindler**, All for One Group, mit einem klaren „Ja“. Sie stellen in ihrem Beitrag **Der integrierte Ansatz bei der Migration in die Cloud: Security by Default** ihre Vorgehensweise für die Cloud-Migration vor, die auf einer vollständig integrierten Sicherheitsarchitektur beruht. Zur Veranschaulichung ihrer Vorgehensweise berichten sie über ein Cloud-Projekt bei einem Maschinenbauer mit dem Ziel, digitale Produkte schnell entwickeln und bereitstellen zu können. Zum Schluss fassen sie ihre Erfahrungen aus Cloud-Projekten zusammen.

Ralf Stadler, Tech Data, erörtert in seinem Beitrag **Sicher in die Cloud** Maßnahmen und Lösungen zur Sicherung von Anwendungen in Public, Multi und Hybrid Clouds. Zunächst begründet er, warum die im eigenen Rechenzentrum genutzten lokalen Security Tools und Sicherheitskonzepte nicht auf das Cloud-Umfeld übertragen werden können, und welche Maßnahmen ergriffen werden sollten. Er beschreibt verschiedene Lösungen beginnend mit der Authentifizierungslösung RSA SecurID und YubiKey sowie mit der IBM-Lösung IBM Cloud Paks for Security, welche sicherheitsrelevante Informationen über alle Datenquellen, Systeme in einem Hybrid-Multi-Cloud-Umfeld automatisiert zusammenführen und auswerten. Er stellt die Microsoft 365 Business Premium-Lösung und weitere Tools vor, die insbesondere KMUs im Remote-Arbeitsumfeld Schutz bieten.

Dominik Birgelen, oneclick, stellt in seinem Beitrag **Anwendungsbereitstellung über die oneclick™ Cloud-Plattform: Ein schlagkräftiges Mittel gegen Cyberkriminalität** die Cloud-Plattform seines Unternehmens vor, welche als Vermittlungs- bzw. Trennschicht zwischen Benutzer und Unternehmensressource fungiert. Streaming-Server dienen als eine Art Sicherheitsschleuse mit Verschlüsselungen und weiteren Sicherheitsmechanismen zwischen Benutzer und Unternehmensressourcen, unabhängig davon, von wem diese bezogen werden. Inkludiert ist eine Cyberversicherung mit vorgeprüften Sicherheitsmaßnahmen ohne vorherige Fallprüfungen beim Anwenderunternehmen.

„Vertrauen ist gut, Kontrolle ist besser“: Das ist das Motto von Zero Trust. Es sieht vor, dass jede einzelne Anfrage und Zugriffe auf Ressourcen als nicht vertrauenswürdig gelten, bis das Gegenteil bewiesen ist. Mit Auflösung des Perimeterschutzes – als klassischer Ansatz für die Netzwerksicherheit – gilt Zero Trust u.a. im Cloud-Umfeld als ein probates Modell, welches auf großes Interesse stößt. **Michael Doujak**, Ergon Informatik, und **Aarno Aukio**, VSHN, erläutern in ihrem Beitrag **Zero Trust ist eine Reise** ein Migrations-Konzept für die Umsetzung einer Zero-Trust-Architektur in Unternehmen. Sie erörtern die technischen und betrieblichen Vorteile einer Zero-Trust-Architektur, zeigen aber auch die Grenzen von Zero Trust auf. Zur stufenweisen Umsetzung dieser Architektur beschreiben sie ein Modell, welches aus einem API-Gateway aus dem Perimeter-schutz – als Aufgabenverteiler zwischen Perimeter und neu eingeführten Microgateways –, Microgateways für den Zero-Trust-Ansatz und einer IAM-Lösung besteht.

Elmar Eperiesi-Beck, eperi, hat den Schwerpunkt seines Beitrages **Datenschutzkonforme Cloud Nutzung – Best Practices für alle Unternehmensgrößen** auf eine datenzentrische Sicht gelegt. „Nicht länger geht es nur um die Sicherheit der Anwendungen. Entscheidend ist der Schutz der darin befindlichen sensiblen Daten“, so der Autor.

Zunächst befasst er sich mit Schutzziele im Kontext mit Cloud-Computing, die die Sicherheit der IT messbar und die aktuelle Gefahrenlage bewertbar machen. Der Autor erläutert die Sicherheitsmaßnahmen der Cloud-Anbieter, die häufig bereits im Angebot integriert sind oder zugebucht werden können. Zur Beurteilung, ob diese Maßnahmen ausreichend sind, führt er Kriterien an, die es bei der Bewertung zu berücksichtigen gilt. Um den Anforderungen an die Datensicherheit und den Datenschutz gerecht zu werden, plädiert er dafür, die Datenverschlüsselung selbst in die Hand zu nehmen. Er erläutert die verschiedenen Arten der Verschlüsselung und führt zum Schluss mehrere Praxisbeispiele an, die durch den Einsatz von Verschlüsselungslösungen datenschutzgerecht umgesetzt werden konnten.

Kritische Infrastrukturen werden als besonders schützenswürdig eingestuft. Durch die zunehmende Digitalisierung werden die Anlagen und Systeme angreifbarer, und die meldepflichtigen IT-Sicherheitsvorfälle haben im letzten Jahr deutlich zugenommen.

Dr. Simon Woldeab, fuentis, gibt in seinem Beitrag **Herausforderungen für Kritische Infrastrukturen (KRITIS)** zunächst einen Überblick über die derzeitige Gesetzeslage und den entsprechenden Richtlinien. Er listet die KRITIS-Sektoren und Anlagenkategorien sowie die entsprechenden Bemessungsgrundlagen und Schwellenwerte auf und erläutert sie. Er geht auf den Anforderungskatalog des BSI ein und diskutiert das Thema „Stand der Technik“ im Zusammenhang mit den branchenspezifischen Sicherheitsstandards (B3S). Zum Schluss veranschaulicht er am Beispiel Krankenhaus den Einsatz eines ISMS unter Einbindung von KRITIS-Standards.

Prof. Dr. Heiko Meyer, KMS Vertrieb und Services, geht in seinem Beitrag **IT-Sicherheit im klinischen Umfeld** darauf ein, warum Kliniksysteme zukünftig als Cloud-Lösung betrieben werden sollten. Er erörtert, warum Hybrid-Cloud-Systeme von Vorteil für Kliniken sind, und gibt Hinweise, wie klinische IT-Systeme sicher in der Cloud betrieben werden können. Dabei werden die gesetzlichen Besonderheiten des Gesundheitswesens näher beschrieben, spezielle Mechanismen zum Schutz der Daten vorgestellt und die daraus resultierenden Vorteile aus betriebswirtschaftlicher und medizinischer Sicht für Patienten, Ärzte, Klinikmanagement sowie Forschung und Wissenschaft erörtert.

Valeri Milke, Insentis, befasst sich in zwei Beiträgen sowohl mit **Best Practices zur automatischen Identifizierung und Behebung der häufigsten kritischen Sicherheitslücken in AWS** als auch mit **Best Practices zur automatischen Identifizierung und Behebung der häufigsten kritischen Sicherheitslücken in Microsoft Azure**. Er legt die Schwerpunkte jeweils auf übergeordnete architektonische Aspekte, auf die wichtigsten sicherheitsbezogenen sowie auf die am häufigsten eingesetzten AWS- und Azure-Services. In tabellarischer Form stellt er den Services detailliert die entsprechenden Handlungsempfehlungen und Maßnahmen gegenüber. Der Autor stellt weitere Tools vor, die die automatisierte Identifizierung von Sicherheitslücken im AWS- und Azure-Umfeld unterstützen. In seinem zweiten Beitrag gibt er zum Abschluss allgemeingültige Hinweise für ein sicheres Cloud Computing.