

Inhaltsverzeichnis

Vorwort	5
Management Abstract	13
Herausforderung Cloud Security: Wandel in Technologie und Organisation.....	
Tino Hirschmann und Marcel Reviol	16
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