

Inhaltsverzeichnis

Geleitwort	V
1 Security: Die echte Herausforderung für die Digitalisierung	1
Ferri Abolhassan	
1.1 Intro	1
1.2 Status quo: Die Cloud ist das Rückgrat der Digitalisierung . . .	2
1.3 Datensicherheit: Nur eine sichere Cloud führt auch zu sicherer Digitalisierung	3
1.3.1 Risiko Transformation: Der Weg in die Cloud muss ein leichter sein	4
1.3.2 Risiko Incident: Damit die Cloud nicht abstürzt	5
1.3.3 Risiko technisch-physischer Angriff: Eine Burgmauer allein reicht nicht	6
1.3.4 Risiko Cyberangriff: Damit Daten und Devices nicht Opfer werden	7
1.4 Blick in die Zukunft	9
1.5 Fazit	10
2 Sicherheitspolitik: Regeln für den Cyberraum	13
Wolfgang Ischinger	
2.1 Bestandsaufnahme: Digitale Kriegsführung im 21. Jahrhundert .	14
2.2 Herausforderungen für die Politik: Regeln, Ressourcen & Expertise	15
2.3 Ausblick: Eine Strategie für das digitale Zeitalter	18

3	Datenschutz-Empowerment	23
	Peter Schaar	
3.1	Code is law	24
3.2	Empowerment	26
3.3	Informationstechnologie und gesellschaftliche Werte	28
4	Red Teaming und Wargaming: Wie lassen sich Vorstände und Aufsichtsräte stärker in das Thema Cyber Security involvieren?	31
	Marco Gercke	
4.1	Cyber Security als Vorstandsthema	31
4.2	Den Vorstand in bestehende Cyber-Security-Strategien einbinden	32
4.3	Red Teaming und Wargaming	32
4.3.1	Definition Red Teaming	32
4.3.2	Definition Wargaming	33
4.3.3	Unterschiede zu aktuell genutzten Methoden	33
4.4	Einsatz von Red Teaming in Kombination mit Wargaming im Unternehmen	34
4.4.1	Systematik	35
4.4.2	Zielsetzung	35
4.4.3	Teamzusammensetzung.	36
4.4.4	Analyse: Sammlung von Informationen und Auswertung . . .	36
4.4.5	Wargaming	37
4.4.6	Bericht	38
4.5	Fazit	38
5	Der Beitrag des Rechts zur IT-Sicherheit: Rechtsrahmen, Anforderungen, Grenzen	41
	Klaus Brisch	
5.1	Zentrale Aspekte des bestehenden Rechtsrahmens	41
5.1.1	IT-Compliance – Herausforderung für Vorstand und Geschäftsleitung	42
5.1.2	Wer ist verantwortlich?	43
5.1.3	Die Verordnung zu Kritischen Infrastrukturen	46
5.1.4	Brisant: Änderungen für Telemediendienste	46
5.2	Internationales: Die NIS-Richtlinie (Netz- und Informationssicherheit) der Europäischen Union	46
5.3	Datenschutz und Datensicherheit in den USA	47
5.4	Datenaustausch zwischen Unternehmen in der EU und den USA	48
5.4.1	Safe Harbor	48

5.4.2	Privacy Shield	48
5.5	Fazit: Reichlich Rechtliches zu beachten	49
6	IT-Sicherheit: Gemeinsam sind wir stärker	53
	Ralf Schneider	
6.1	Die Dreifaltigkeit der IT-Sicherheit	53
6.2	CSSA – Sicherheit durch Zusammenarbeit	55
6.2.1	Zielgerichtete Interaktion	56
6.2.2	Network of Trust	56
6.3	Die sechs Stufen der ganzheitlichen Abwehrstrategie	57
6.3.1	Vorsorge ist die beste Medizin	58
6.3.2	Wissen ist Macht	59
6.3.3	IT-Sicherheit ist kein Selbstzweck	60
6.3.4	Ein Tag wird kommen: Die Rolle von Incident Management	61
6.3.5	Für den Ernstfall fitmachen	62
6.3.6	Gemeinsam geht es besser	62
6.4	Fazit	63
7	Deutscher Security-Markt: Auf der Suche nach den Rundum-sorglos-Diensten	65
	Markus a Campo, Henning Dransfeld, Frank Heuer	
7.1	Die Herausforderungen für IT-Security-Verantwortliche	65
7.2	Schutz – aber wie? Ein zersplittertes Angebot	66
7.2.1	Data Leakage / Loss Prevention (DLP)	67
7.2.2	Security Information und Event Management (SIEM)	67
7.2.3	E-Mail / Web / Collaboration Security	67
7.2.4	Endpoint Security	68
7.2.5	Identity und Access Management (IAM)	68
7.2.6	Mobile Security – ist der Mitarbeiter wirklich das größte Risiko?	69
7.2.7	Network Security	70
7.2.8	Fazit	71
7.3	Sicherheit aus einer Hand – Managed Security Services	71
7.3.1	Managed Service versus Cloud-Lösung	72
7.3.2	Auswahlkriterien	73
7.3.3	Bewertung der Deutschen Telekom / T-Systems als Managed-Security-Services-Anbieter	73
7.3.4	Spezielle Managed Security Services	75

8	CSP statt 007: Integrierte Qualifizierung im Bereich Cyber Security . .	79
	Rüdiger Peusquens	
8.1	Neues Berufsbild Cyber Security Professional: Vom ITler zum IT-Sicherheitsexperten	79
8.2	Praxiseinsatz in allen Sicherheitsbereichen	80
8.3	Cyber-Security-Fachwissen auch für Manager	81
8.4	Fazit	81
9	Menschliche Faktoren in der IT-Sicherheit	85
	Linus Neumann	
9.1	IT-Sicherheit ist oft nicht für Menschen geschaffen	85
9.1.1	Die Sache mit den Passwörtern	85
9.1.2	„Falsche“ IT-Sicherheit ist der Gegner unserer Produktivität	87
9.2	Social Engineering	87
9.3	Menschliche „Schwachstellen“ sind oft soziale Normen oder simple Instinkte	89
9.3.1	Könnten Sie bitte diese Malware auf Ihrem Rechner installieren?	89
9.3.2	Entschuldigung, wie lautet denn Ihr Passwort?	91
9.4	Können Sie mir bitte ein paar Millionen Euro überweisen?	92
9.5	Schutzmaßnahmen	93
9.5.1	Social Engineering erkennen	94
9.5.2	Lernziel: Verdächtige Vorgänge melden	95
9.5.3	Übung macht den Meister	96
9.6	Fazit: IT muss für und nicht gegen die Nutzer arbeiten	96
10	Sicher und einfach: Security aus der Steckdose	99
	Dirk Backofen	
10.1	Datensicherheit im roten Bereich	100
10.2	Digitalisierung benötigt neue Sicherheitskonzepte	103
10.3	Digitale Identität ist die neue Währung	104
10.4	Gibt es einen absoluten Schutz?	105
10.5	So sehen Angriffsszenarien heute aus	106
10.6	Security-Baustelle Mittelstand	107
10.7	Teuer ist nicht gleich sicher: Security-Lücken in Großunternehmen	108
10.8	Gütesiegel „Made in Germany“	109
10.9	Unternehmen wollen die Cloud – aber sicher	110

11	Cyber Security – What’s next?	113
	Thomas Tschersich	
	11.1 Motive der Angreifer mit jeder Generation böswilliger	113
	11.2 Cyber Security – der schlafende Riese in Unternehmen	118
	11.3 Was wird uns schützen?	121
	11.4 Fazit	123
12	Fazit	127
	Ferri Abolhassan	
	12.1 Nichts geht mehr ohne das Internet	127
	12.2 Gutes Internet, böses Internet	128
	12.3 Cyber-Hase vs. Cyber-Igel	128
	12.4 „Einfach und sicher“ heißt die Devise	130
	Anhang	133
	Glossar	139