

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Motivation und Zielsetzung	1
1.2	Forschungsfragen	3
1.3	Forschungsmethodik	4
1.4	Aufbau der Arbeit	4
<b>2</b>	<b>Begriffe, Grundlagen und Bezugsrahmen</b>	<b>7</b>
2.1	Quantifizierung und Metriken	7
2.2	Sicherheit	8
2.2.1	IT-Sicherheit und Informationssicherheit	8
2.2.2	Schutzziele	9
2.2.3	Mehrseitige Sicherheit	10
2.2.4	Angreifermodelle	10
2.2.5	Vertrauen	11
2.3	Sicherheitsmanagement	11
2.3.1	Informationssicherheitsmanagement	11
2.3.2	Informationssicherheitsmanagementsystem (ISMS)	13
2.4	Risiko und Risikomanagement	15
2.4.1	Risikobegriff	15
2.4.2	Risikomanagement	17
2.5	Begriffsmodell	18
2.5.1	Assets	18
2.5.2	Schwachstellen	19
2.5.3	Angreifer und Angriff	20
2.5.4	Bedrohungen	20
2.5.5	Sicherheitsvorfälle	20
2.5.6	Management von Sicherheitsvorfällen	21
2.5.7	Schaden	22
2.5.8	Sicherheitsmaßnahmen	22
2.5.9	Beispiel	23
2.6	Kosten und Nutzen von Informationssicherheit	24
2.7	Ökonomische Aspekte der Informationssicherheit	25
<b>3</b>	<b>Informationssicherheitsmanagement als Risikomanagementaufgabe</b>	<b>29</b>
3.1	Einflüsse auf das Informationssicherheitsmanagement	29
3.1.1	IT-Abhängigkeit und Bedrohungslage	29
3.1.2	Wirtschaftlichkeitsgebot	31

3.1.3	IT-Governance und IT-Compliance . . . . .	33
3.1.4	Internationale Standards und Normen . . . . .	40
3.2	Management von Informationssicherheitsrisiken . . . . .	43
3.2.1	Standards und Vorgehensmodelle . . . . .	44
3.2.2	Phasen des Risikomanagementkreislaufs . . . . .	47
3.2.3	Klassifikation von Werkzeugen und Methoden . . . . .	53
<b>4</b>	<b>Einsatz quantitativer Daten für das Risikomanagement</b>	<b>57</b>
4.1	Notwendigkeit quantitativer Daten . . . . .	57
4.2	Risikomaße . . . . .	59
4.2.1	Jährliche Verlusterwartung . . . . .	59
4.2.2	Value at Risk . . . . .	63
4.2.3	Ermittlung der Verlustverteilung . . . . .	65
4.2.4	Sonstige Ansätze . . . . .	67
4.2.5	Weitere Anwendungsmöglichkeiten . . . . .	67
4.2.6	Fazit . . . . .	69
4.3	Metriken und Regeln zur Risikosteuerung . . . . .	69
4.3.1	ROSI-basierte Konzepte . . . . .	69
4.3.2	Nettokapitalwert-basierte Konzepte . . . . .	73
4.3.3	Anwendungshinweise und Fazit . . . . .	75
4.4	Quellen für quantitative Daten . . . . .	76
4.4.1	Verfügbarkeit quantitativer Daten . . . . .	77
4.4.2	Mögliche Quellen . . . . .	78
4.4.3	Fazit . . . . .	86
4.5	Empirische Überprüfung des Status Quo . . . . .	86
4.5.1	Untersuchungsdesign und Vorgehen . . . . .	86
4.5.2	Ergebnisse und Implikationen . . . . .	88
<b>5</b>	<b>Grundkonzept eines überbetrieblichen Vorfallsdatenaustauschs</b>	<b>93</b>
5.1	Notwendigkeit historischer Daten . . . . .	93
5.2	Basiskonzept . . . . .	95
5.2.1	Zu erfassende Vorfallsdaten . . . . .	95
5.2.2	Architektur und Akteure . . . . .	96
5.2.3	Aufgaben der zentralen Plattform . . . . .	97
5.2.4	Auswertungsmöglichkeiten . . . . .	98
5.3	Nutzenbetrachtung . . . . .	99
5.3.1	Direkte Effekte auf Ebene der Einzelorganisation . . . . .	99
5.3.2	Aus Marktmodellen abgeleitete Effekte . . . . .	100
5.3.3	Übergreifende Aspekte . . . . .	102
5.4	Abgrenzung zu existierenden Ansätzen . . . . .	103
5.4.1	CERTs und CSIRTs . . . . .	104
5.4.2	Information Sharing Analysis Centers (ISACs) . . . . .	105
5.4.3	Internet Storm Center (ISC) . . . . .	106
5.4.4	Carmentis . . . . .	106
5.4.5	Leurrecom.org Honeynet Project . . . . .	107

5.4.6	mwcollect Alliance	108
5.4.7	Sonstige verwandte Initiativen	108
5.4.8	Fazit	109
5.5	Empirische Evaluation des Basiskonzepts	110
<b>6</b>	<b>Anforderungen und Lösungen</b>	<b>113</b>
6.1	Ergebnisaufbereitung	113
6.1.1	Auswertungen für die Risikobewertung	114
6.1.2	Selektionskriterien	116
6.1.3	Arten der Ergebnisdarstellung	117
6.1.4	Formen der Datenbereitstellung	117
6.1.5	Weitere Auswertungsmöglichkeiten	120
6.1.6	Fazit	123
6.2	Vergleichbarkeit der Vorfälle	123
6.2.1	Problemstellung und Anforderungen	123
6.2.2	Bestehende Klassifikationskonzepte für Sicherheitsvorfälle	127
6.2.3	Taxonomie zur Vorfallsbeschreibung	140
6.2.4	Erfassung der Schäden/Auswirkungen	143
6.2.5	Erfassung relevanter Organisationsparameter als Bezugsgrößen	149
6.2.6	Fazit und mögliche Erweiterungen	152
6.3	Sicherheit	154
6.3.1	Grundmodell	154
6.3.2	Erweiterung 1 – Teilnehmer als Angreifer auf technischer Ebene	160
6.3.3	Erweiterung 2 – Teilnehmer als Angreifer auf inhaltlicher Ebene	162
6.3.4	Erweiterung 3 – Minimales Vertrauen in den Plattformbetreiber	170
6.3.5	Fazit	180
6.4	Fairness	181
6.4.1	Fairness und kooperatives Verhalten	182
6.4.2	Free-Riding-Problem	183
6.4.3	Truth-Telling-Problem	185
6.4.4	Ansätze zur Verhinderung unfairen Verhaltens	188
6.4.5	Bausteine eines Anreizsystems	192
6.5	Fazit	196
<b>7</b>	<b>Prototyp</b>	<b>199</b>
7.1	Zielsetzung	199
7.2	Technisches Konzept und Systemarchitektur	200
7.3	Umsetzung der Anforderungen aus Kapitel 6	203
7.3.1	Auswertungen und Reports	203
7.3.2	Abbildung der Taxonomie	204
7.3.3	Sicherheitskonzept	206
7.3.4	Anreizsystem	209
7.3.5	Minimierung des Aufwands	210
7.4	Ausgewählte Funktionalitäten der Anwendung	211
7.5	Integration weiterer Datenquellen	212

7.6	Bewertung und Erweiterungsmöglichkeiten . . . . .	213
<b>8</b>	<b>Integration in die Organisation</b>	<b>217</b>
8.1	Definition eines Incident Reporting Prozesses . . . . .	217
8.1.1	Status Quo der Behandlung von Sicherheitsvorfällen . . . . .	217
8.1.2	Erweiterter Prozess zur Behandlung von Sicherheitsvorfällen . . . . .	218
8.1.3	Rollen und Datenquellen . . . . .	220
8.2	Integration in den Risikomanagementprozess . . . . .	222
8.2.1	Risikoidentifikation . . . . .	223
8.2.2	Risikobewertung . . . . .	225
8.2.3	Risikosteuerung . . . . .	229
8.2.4	Risiküberwachung . . . . .	230
8.2.5	Fazit . . . . .	231
8.3	Bezüge zum Business Engineering . . . . .	232
<b>9</b>	<b>Zusammenfassung und Ausblick</b>	<b>237</b>
9.1	Überprüfung der Forschungsfragen . . . . .	237
9.2	Anregungen für die zukünftige Forschung . . . . .	240
9.3	Ausblick . . . . .	243
	<b>Anhang</b>	<b>245</b>
A	Interviewleitfaden	249
B	Taxonomien für Informationssicherheitsvorfälle	253
C	Begriffsmodell zur Vorfallerfassung	259
D	Systematik zur Schadenserfassung	272
	Literaturverzeichnis	275
	Referenzierte Standards	301