
Inhaltsverzeichnis

1	Cyber-Krisen wie aus dem Lehrbuch	1
1.1	Cyber Crisis re-invented: Sony Pictures Entertainment.	1
1.2	Dramaturgie unzureichend gemanagter Cyber-Krisen	3
2	Menschen und andere Crown Jewels	9
2.1	Crown Jewels – oder: Wie wir Schwerpunkte setzen	9
2.2	Faktor Mensch	11
2.2.1	Entscheidungen oder die Essenz von Krisenbewältigung	11
2.2.2	Bewertungen, Verhaltensmuster und Stress	13
2.2.2.1	Wie Menschen Situationen wahrnehmen und bewerten	13
2.2.2.2	Verhaltensmuster und wie sie sich äußern	14
2.2.2.3	Stress und wie er entsteht	15
2.2.2.4	Stress und was wir dagegen tun können	17
2.2.3	Anforderungen an die Mitglieder der Krisenorganisation	20
3	Cyber Crisis Response	23
3.1	Executive Summary: Crown-Jewels-basierte Cyber Crisis Response	23
3.2	Alarmierung, Eskalation und Benachrichtigung	26
3.2.1	Grundsätze und Erfolgsfaktoren	26
3.2.2	Verantwortlichkeiten und Abläufe	30
3.2.3	Erreichbarkeits- oder Bereitschaftsregelung	33
3.2.4	Informationskanäle oder: Alarmierungstools vs. Telefonkaskaden	34
3.2.5	Eskalationskriterien vs. Verantwortungsfreude und Fehlerkultur	37
3.3	Reaktion auf strategischer Ebene	39
3.3.1	Die Weichen stellen: Initialisierung der Krisenstabsarbeit	39
3.3.1.1	Bevor wir zur Tat schreiten: Die „Du-kommst aus-dem-Gefängnis-frei-Karte“	40
3.3.1.2	Erste Lagefeststellung oder: Was ist überhaupt los?	44

3.3.1.3	Betroffene Stakeholder oder: Mit wem müssen wir rechnen?	46
3.3.1.4	Ausnahmsweise mal negativ denken: Was wäre wenn?	54
3.3.1.5	Von der Feststellung zur Beurteilung: Ziel, Ziel und nochmals Ziel.	58
3.3.1.6	Die formale Feststellung des Krisenfalls: Houston, wir haben ein Problem.	63
3.3.2	Cyber-Krisen strukturiert bewältigen: Krisenbewältigungsprozess	64
3.3.2.1	Die Qual der Wahl: Nach welchem Schema wollen wir arbeiten?	65
3.3.2.2	Deep Dive: Bewältigungsprozess auf strategischer Ebene	66
3.3.2.2.1	Lagebewertung: Wo drückt der Schuh am meisten?	68
3.3.2.2.2	Handlungsfelder und -optionen: Was tun, sprach Zeus?	69
3.3.2.2.3	Entscheidung und Delegation: Nicht reden, handeln!	70
3.3.2.2.4	Lagefeststellung/Überprüfung: Wirkt es schon?	72
3.3.3	Krisenkommunikation	74
3.3.3.1	Faustregeln für die Krisenkommunikation	75
3.3.3.2	Ausgangspunkt: Bedürfnisse und Nöte der Stakeholder in Cyber-Krisen	76
3.3.3.3	W-Fragen der Krisenkommunikation	79
3.3.3.3.1	Wer kommuniziert mit wem?	79
3.3.3.3.2	Was kommunizieren wir?	80
3.3.3.3.3	Wie kommunizieren wir (hoffentlich)?	82
3.3.3.3.4	Wann kommunizieren wir?	84
3.3.3.4	Von Bloggern, YouTubern und Journalisten: Grenzen des Presserechts	85
3.3.4	Aus der Praxis: Strategien und Taktiken in akuten Cyber-Krisen	86
3.3.4.1	Victim Care über alles	87
3.3.4.2	Wir sind selbst auch Opfer!	89
3.3.4.3	Angriff ist die beste Verteidigung	92
3.3.4.4	Die Karten auf den Tisch legen vs. Kommunikationsverweigerung	94
3.3.4.5	Den Kopf aus der Schlinge ziehen oder aus der Schusslinie verschwinden	95

3.3.4.6	Einen Sündenbock gegen eine Identifikationsfigur tauschen	97
3.3.4.7	Wenn wir erpresst werden	98
3.3.4.8	Die juristische Keule schwingen	100
3.4	Reaktion auf taktisch-operativer Ebene	102
3.4.1	Die Show muss weitergehen oder: Wiederanlauf von Prozessen und IT-Systemen.	102
3.4.1.1	Wiederanlauf: kritische (Geschäfts-)Prozesse	104
3.4.1.2	Wiederanlauf: IT-Systeme und Daten	106
3.4.2	Cybersecurity Incident Response	112
3.4.2.1	Cybersecurity Incident Response	114
3.4.2.2	Faustregeln bei der Cybersecurity Incident Response	116
4	Cyber Crisis Preparation	119
4.1	Executive Summary: Crown Jewels basierte Cyber Crisis Preparation	119
4.2	Nichts für die Linie oder: Notfall- und Krisenorganisation	123
4.2.1	Die Rettungsmannschaft oder: der Krisenstab	124
4.2.1.1	Der organisatorische Rahmen des Krisenstabs	126
4.2.1.2	Zusammensetzung des Krisenstabs	128
4.2.1.3	Gretchenfrage: Wer (besser nicht) Mitglied des Krisentabs sein sollte	132
4.2.2	Lagezentrum	134
4.2.3	Kommunikationsstab	135
4.2.4	Notfallgremien der taktisch-operativen Ebene	137
4.3	Hilfsmittel	139
4.3.1	Krisenhandbuch	139
4.3.2	Krisenstabsraum	143
4.3.3	Templates, Poster und Vorlagen	145
4.3.4	IT-gestützte Krisenmanagement-Tools	146
4.3.5	Alarmierungstools	149
4.3.6	Governance-Suiten für BCM, IRBC und ISM	150
4.3.7	Tools zur Detektion von und Reaktion auf Angriffe	151
4.4	Logistik sichert Durchhaltefähigkeit	153
4.5	Vorbereitung der Krisenkommunikation	155
4.5.1	Rechtzeitig die Hausaufgaben machen	155
4.5.2	Kommunikationshilfen	157
4.6	Es ist noch kein Meister vom Himmel gefallen: Trainings und Übungen	162
4.6.1	Formate	162
4.6.2	Trainingsprogramm	164
4.7	Voraussetzungen für die Fortsetzung des Geschäftsbetriebs schaffen	167

4.7.1	Notbetrieb der (Geschäfts-)Prozesse vorbereiten: Geschäftsfortführungspläne	169
4.7.2	Wiederanlauf der IT-Systeme ermöglichen	171
4.7.2.1	Technische Lösungen.	171
4.7.2.2	Organisatorische Vorbereitungen: Playbooks, Wiederanlaufpläne und Restore-Konzepte	172
4.7.3	Rahmenbedingungen für Cybersecurity Incident Response schaffen	176
4.8	Was funktioniert und was nicht: Tests	176
4.9	Versicherung von Cyberrisiken	181
5	Cyber Crisis Prevention	185
5.1	Executive Summary: Crown Jewels basierte Cyber Crisis Prevention	185
5.2	Bevor wir losfahren: IT-Sicherheitsarchitektur und drei Prinzipien	187
5.2.1	(Privileged) Access Management.	188
5.2.2	Weitere Pfeiler der IT-Sicherheitsarchitektur.	189
5.3	(Früh-)Warnsystem: Gefahr erkannt, Gefahr gebannt	192
5.3.1	Issue Management	192
5.3.2	Awareness.	193
5.3.3	Threat Intelligence	195
5.3.4	Logging, Monitoring, Alerting	198
5.4	Unverzichtbar: Information und IT Security Management	200
5.5	Cyber Risk Management	201
5.5.1	Vorarbeiten	202
5.5.2	Risk Assessment.	203
5.5.2.1	Risikoidentifikation	203
5.5.2.2	Risikoanalyse.	205
5.5.2.3	Risikobewertung	207
5.5.3	Risikobehandlung.	208
5.5.4	Akzeptanz von (Rest-)Risiken	210
5.6	Unsere Cyber Resilience und wie es um sie bestellt ist: Audits und Assessments	211
6	Cyber Crisis (& Security) Grundlagen	215
6.1	Executive Summary: Crown Jewels	215
6.2	Geht auch ohne, aber dann wird's halt...: Informationssicherheitsstrategie	216
6.3	Ordnung im Chaos: Kritikalitäten und Abhängigkeiten	217
6.3.1	Ermittlung von Business Impact und Schutzbedarfen, oder: schon wieder Crown Jewels	218
6.3.2	Asset Management und Strukturanalyse, oder: Welche Fleißarbeit müssen wir leisten?	222

6.4	Integration von Stakeholdern, oder: Macht denn hier jeder, was er will?	225
6.4.1	Stakeholder und ihre Issues	225
6.4.2	Risikokommunikation (und ihre Tücken)	228
6.4.3	3rd Party Risk & Provider Management	231
6.4.4	Governance.	234
7	Post Crisis Care – Krisennachsorge und -nachbereitung	237
7.1	Executive Summary: Crown Jewels basierte Post Crisis Care.	237
7.2	Der Blick nach außen: Reparieren der Stakeholderbeziehungen.	238
7.3	Der Blick nach innen: Menschen, Abläufe und Technik	239
7.3.1	Faktor Mensch	240
7.3.2	Crown Jewels	242
7.3.3	Alarmierung und Eskalation.	242
7.3.4	Zusammenspiel der Ebenen der Notfall- und Krisenorganisation	243
7.3.5	Strategische Ebene	243
7.3.6	Taktische Ebene: BCM und IRBC	245
7.3.7	Operative Ebene: Cybersecurity Incident Response	246
7.3.8	Krisenkommunikation	247
7.3.9	Prävention, Cyberhygiene und Dienstleistersteuerung	248
8	Auf einen Blick: Sieben Todsünden des Cyber Crisis Managements	249
	Zum Weiterlesen	253
	Abkürzungen und Glossar	259