

Kommunikation in der Cyberkrise

Sprach- und handlungsfähig im IT-Ernstfall

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

1	Einleitung	19
<hr/>		
	Teil I: Der Einstieg	29
2	Case Study: Compor AG	31
3	Historische Beispiele	51
<hr/>		
	Teil II: Background – Grundlagen von Cyberkrisen	65
4	Anatomie einer Cyberkrise	67
5	Vorbereitung und Risikoanalyse	91
6	Analyse von Cyberkrisen	109
7	Recht und Regulierung	135
8	Grundlagen und Prinzipien der Krisenkommunikation	145
9	Kommunikation bei Cyberkrisen	155
<hr/>		
	Teil III: Der Werkzeugkasten – Reaktion auf die Krise	171
10	Kickstart Krisenmanagement	173
11	Rollen und Verantwortlichkeiten	205
12	Interne Kommunikation	213

13 Externe Kommunikation	225
14 Digitale Kanäle und Social Media	239
15 Medienarbeit in der Cyberkrise	255
16 Wer darf was wann wissen? – Vertraulichkeit, Geheimhaltung und Informationsaustausch	277
17 Kommunikation mit Angreifern	285
<hr/>	
Teil IV: Gute Vorbereitung	307
18 Toolbox für die Praxis	309
19 Training und Übungen	325
<hr/>	
Teil V: Nachbereitung und Ausblick	349
20 Analyse und Nachbereitung	351
21 Die Cyberkrisenkommunikation von morgen: Von der Reaktion zur Resilienz	361
A Glossar	369
B Literaturverzeichnis	373
Index	377

1	Einleitung	19
	Orientierung in digitalen Ausnahmesituationen: Warum es dieses Buch braucht	20
	An wen sich das Buch richtet	21
	Wie Sie mit dem Buch arbeiten	23
	Schnellstart für Eilige – die wichtigsten Kapitel für den schnellen Einstieg	26
	Die Website zum Buch	27
<hr/>		
	Teil I: Der Einstieg	29
2	Case Study: Compor AG	31
	Die Firma	31
	Standorte	32
	Mitarbeitende	33
	Chronologie einer Krise – vom ersten Verdacht bis zur Aufarbeitung ...	36
3	Historische Beispiele	51
	Wenn man nicht kommuniziert – Deutscher Bundestag	52
	Wenn man verharmlost – Equifax	54
	Wenn man nicht zuhört – die Connect17-App der CDU	55
	Wenn man Insidern glaubt – Tesla	56
	Wenn man Patches vernachlässigt – Universitätsklinikum Düsseldorf ...	58
	Wenn man sich zu viel Zeit lässt – SolarWinds	59
	Wenn man falsch verstanden wird – Kammergericht Berlin	60
	Wenn man sich die Öffentlichkeit zum Freund macht – Facebook	63

Teil II: Background – Grundlagen von Cyberkrisen	65
4 Anatomie einer Cyberkrise	67
Was eine Cyberkrise ausmacht – Definition, Abgrenzung, Relevanz ...	67
Elemente einer Cyberkrise – vom Angreifer bis zur Auswirkung	72
Verursacher – wer steckt hinter dem Problem?	74
Motivation – zwischen Macht und Missgeschick	77
Root Cause – wie Vorfälle entstehen	79
Betroffene Systeme – wo Vorfälle entstehen	82
Auswirkungen – wenn nichts mehr geht	85
Betroffene Personen und Organisationen – wen die Krise betrifft ...	87
Wie alles zusammenhängt – systemische Dynamiken verstehen	88
5 Vorbereitung und Risikoanalyse	91
Bedrohungen einschätzen – Risikoanalyse und Modellierung	91
Risikobereitschaft als Faktor – Entscheiden im Spannungsfeld	96
Strategien zur Risikominimierung – was Sie präventiv tun können	99
ISO 27001	100
Grundschutz nach BSI	102
NIST CSF	103
Welches Framework eignet sich wofür?	108
6 Analyse von Cyberkrisen	109
Identifikation	110
Erste Einschätzung	114
Beispiel 1	114
Beispiel 2	116
Die Cyber Kill Chain® – Phasen eines Angriffs verstehen	117
MITRE ATT&CK® – Taktiken, Techniken und Verfahren	123
Das Diamond Model – Beziehungen innerhalb eines Angriffs verstehen	129
Dreifach stark – der kombinierte Einsatz von Analysemodellen	132
Die Gefahr von Fehlannahmen sinkt	132
Die Dynamik von Angriffen wird berücksichtigt	133
Kein Vertrauensverlust durch ungenaue Kommunikation	133
Fazit	133
7 Recht und Regulierung	135
Relevante Gesetze und Normen	135
Datenschutz und Meldepflichten	140
Datenschutzbeauftragte	143

8 Grundlagen und Prinzipien der Krisenkommunikation	145
Definition und Ziele der Krisenkommunikation	145
Kommunikationsstrategien in einer Krise	149
Faktor Mensch	150
Krisentypen und Kommunikationsstrategien	152
9 Kommunikation bei Cyberkrisen	155
Was Cyberkrisen besonders macht	155
Weitere kommunikative Herausforderungen – Umgang mit Komplexität	159
Praktische Herausforderungen	160
Taktische Herausforderungen	161
Entwicklung eines Krisenkommunikationsplans	163
Kommunikation mit technischen Experten – zwischen Welten übersetzen	167
<hr/>	
Teil III: Der Werkzeugkasten – Reaktion auf die Krise	171
10 Kickstart Krisenmanagement	173
Ein 10-Punkte-Plan für Sofortmaßnahmen am IT-Unfallort, wenn’s richtig brennt	173
1. Identifizieren Sie die Art des Incidents!	174
2. Formieren und organisieren Sie einen Krisenstab!	178
Der Krisenstabsleiter	178
Das Lage-Team	179
Das Fach-Team	180
Arbeitsweise	181
3. Bereiten Sie frühzeitig die Kommunikation vor!	182
Kommunikation mit Behörden	182
Interne Kommunikation	183
Externe Kommunikation	187
4. Sichere Kommunikationskanäle sind unverzichtbar!	188
Telefonieren	188
E-Mail	189
Messenger-Dienste	190
Austausch von Dateien	190
Internetzugang	190
Die Unternehmenswebsite	191
Kommunikation zwischen den Beteiligten	192
5. Lassen Sie alles in Sicherheit bringen, was geht!	193
6. Dokumentation sofort starten!	195

7. Holen Sie frühzeitig Experten dazu!	196
8. Prioritäten setzen!	199
9. Entscheidungen treffen	202
10. Ruhe bewahren!	203
11 Rollen und Verantwortlichkeiten	205
Teamstruktur in der Krise	205
Schnittstellen verstehen und nutzen – Kommunikation ohne Reibungsverluste	208
12 Interne Kommunikation	213
Informieren und Mobilisieren der Mitarbeitenden	213
Menschen als Kommunikatoren	216
Menschen als Entscheidungsträger	217
Menschen als Multiplikatoren	217
Menschen als emotionale Wesen	217
Wenn die Krise ins Herz trifft: Menschliche Resilienz stärken	218
Kommunikationswege unter Beschuss: So bleiben Teams verbunden	220
Stufe 1: Das Intranet ist kompromittiert	221
Stufe 2: Intranet und E-Mail sind kompromittiert	222
Stufe 3: Intranet, E-Mail und Messenger sind kompromittiert	222
Stufe 4: Intranet, E-Mail, Messenger und Telefon sind kompromittiert	222
Stufe 5: Totalausfall aller digitalen und elektronischen Systeme	223
13 Externe Kommunikation	225
Kommunikation mit Kunden, Partnern und der Öffentlichkeit	225
Zusammenarbeit mit Medien und Behörden	231
Medien	231
Behörden	236
14 Digitale Kanäle und Social Media	239
Social Media Monitoring und Sentiment-Analyse	239
Social Media Monitoring	240
Sentiment-Analyse	243
Echtzeit-Kommunikation auf digitalen Plattformen	247
Phasen der Kommunikation in der akuten Krise	249
Die »Luftbrücke« – der Informationsfluss zwischen IT und Kommunikation	250
Die Wahl der richtigen Plattform	252

15 Medienarbeit in der Cyberkrise	255
Pressemitteilungen und Stellungnahmen	255
Pressekonferenzen	258
1. Akt: Die Exposition – die Entscheidung zur Pressekonferenz	259
2. Akt: Die Vorbereitung – Skript, Rollen und (wenn genügend Zeit vorhanden ist) Proben	260
3. Akt: Der Höhepunkt – der Gang vor die Presse	260
4. Akt: Der Abgang – Kontrolle bewahren	261
5. Akt: Die Nachbereitung – Kritik, Learnings, Anpassung	261
Die Wahl des Sprechers	262
Analoge versus virtuelle Pressekonferenzen	263
Umgang mit Medienanfragen	264
Verschiedene Formen von Medienanfragen	268
Entscheidung über Form und Umfang der Reaktion	270
Strategien bei fehlerhafter Berichterstattung	272
Sonderfall Fake News	274
Die Rolle des Presserechts in der Cyberkrisenkommunikation	275
16 Wer darf was wann wissen? – Vertraulichkeit, Geheimhaltung und Informationsaustausch	277
Das VS-Einstufungssystem	279
Das Traffic Light Protocol	280
Unter eins, zwei, drei	282
Firmeninterne Regelungen	284
17 Kommunikation mit Angreifern	285
Die Ökonomie der Erpressung	285
Wer sind die Angreifer?	286
Wie sind die Angreifer organisiert?	287
Warum tun sie, was sie tun?	288
Vorbereitende Maßnahmen	289
Verhandlungsansätze und Taktiken	292
Schlüsselfaktoren einer Ransomware-Verhandlung	295
»Freundliche« Angreifer? – Mythos und Realität	298
(Straf-)Rechtliche Aspekte	299
Mache ich mich strafbar, wenn ich zahle?	299
Cyberversicherung kontaktieren	301
Externe Spezialisten für die Verhandlungsführung hinzuziehen	301
Umgang mit Stress und Druck	302
Warum Erpresser nicht unbegrenzt Zeit haben	303
Taktische Maßnahmen: So kehren Unternehmen den Druck um	303

Zwischen Stakeholder-Transparenz und taktischer Verhandlungsführung	305
Das Dilemma der parallelen Kommunikation	305
Taktische Kommunikation: Ein Balanceakt zwischen Wahrheit und Strategie	306

Teil IV: Gute Vorbereitung **307**

18 Toolbox für die Praxis **309**

A Checkliste zur Dokumentation von Verdachtsmomenten	310
B Muster für einen Krisenkommunikationsplan	312
C Modulbaukasten für Pressemitteilungen	315
D Selbst-Check: Wo steht meine Organisation?	317
E Die CR-Karte: Spreche ich wirklich mit dem CEO?	320

19 Training und Übungen **325**

Krisenübungen durchführen – Simulation statt Improvisation	325
Übungsszenarien	328
1. Szenario: »Der stille Abfluss«	328
2. Szenario: »Lieferstopp«	329
3. Szenario: »Gefälschte Lieferkette«	330
4. Szenario: »Backups? Welche Backups?«	331
5. Szenario: »Der CEO ist gar nicht der CEO«	333
6. Szenario: »Update mit Nebenwirkungen«	334
7. Szenario: »Spion im Smartphone«	335
8. Szenario: »Shitstorm nach dem Cyberangriff«	336
9. Szenario: »Überflutung im Rechenzentrum«	337
10. Szenario: »Schlechter Fisch, kein Patch«	338
11. Szenario: »Anpfeif blockiert«	339
Übungen als Frühwarnsystem – Lücken erkennen, Lösungen schaffen	340
Entscheidungen und Kommunikation unter Stress	342
Was wir von der Luftfahrt über den Umgang mit Cyberkrisen lernen können	343
Welche Implikationen ergeben sich daraus für die Kommunikation in der Cyberkrise?	345
Verhaltensmuster in der Krise: Wie Menschen unter Stress agieren	346
Wie sollte man mit diesen Verhaltensmustern umgehen?	348

Teil V: Nachbereitung und Ausblick	349
20 Analyse und Nachbereitung	351
Dokumentation und Auswertung des Krisenverlaufs	351
Root-Cause-Analyse: Ursachen hinterfragen statt Symptome beheben	352
Analyse der Kommunikation	353
Lessons Learned und Verbesserungsmaßnahmen	355
Bewertung der Kommunikation in der Krise	356
21 Die Cyberkrisenkommunikation von morgen: Von der Reaktion zur Resilienz	361
Ein Wettlauf zwischen Angriff und Verteidigung	361
Cyberkrisen: Ein Flächenphänomen	363
Wer ist besonders gefährdet?	364
Neue Bedrohungen durch KI	365
Handlungsempfehlungen: Wie können Unternehmen sich schützen?	365
Herausforderungen für die Kommunikation	366
A Glossar	369
B Literaturverzeichnis	373
Index	377