

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>xix</b>
Wer sollte dieses Buch lesen? . . . . .	xx
Wie dieses Buch aufgebaut ist . . . . .	xxi
Weitere Elemente. . . . .	xxiii
Bleiben Sie auf dem neuesten Stand . . . . .	xxiv
<b>Danksagungen</b>	<b>xxv</b>
<b>1 Auswirkungen</b>	<b>1</b>
1.1 Eine Cyberepidemie . . . . .	4
1.2 Was ist Cybererpressung? . . . . .	5
1.2.1 Die CIA-Triade . . . . .	5
1.2.2 Arten digitaler Erpressung . . . . .	6
1.2.3 Multikomponenten-Erpressung . . . . .	7
1.3 Auswirkungen moderner digitaler Erpressung . . . . .	8
1.3.1 Betriebsunterbrechung . . . . .	8
1.3.2 Finanzielle Einbußen . . . . .	10
1.3.3 Reputationsverlust . . . . .	14
1.3.4 Gerichtsverfahren. . . . .	14
1.4 Wahl der Opfer . . . . .	17
1.4.1 Opportunistische Angriffe . . . . .	17
1.4.2 Gezielte Angriffe . . . . .	19
1.4.3 Hybride Angriffe . . . . .	20
1.5 Verbreitung . . . . .	20
1.5.1 Managed Services Provider . . . . .	20
1.5.2 Technologiehersteller . . . . .	22
1.5.3 Softwareschwachstellen . . . . .	23
1.5.4 Cloud-Anbieter . . . . .	24

---

1.6	Fazit .....	27
1.7	Sie sind dran! .....	27
<b>2</b>	<b>Evolution</b> .....	<b>29</b>
2.1	Herkunftsgeschichte .....	30
2.2	Kryptovirale Erpressung .....	32
2.3	Frühe Erpresser-Malware .....	33
2.4	Wesentliche technische Fortschritte .....	34
2.4.1	Asymmetrische Kryptografie .....	34
2.4.2	Kryptowährungen .....	38
2.4.3	Onion-Routing .....	40
2.5	Ransomware wird Mainstream .....	41
2.6	Ransomware-as-a-Service .....	43
2.7	Enthüllung .....	44
2.8	Doppelerpressung .....	46
2.9	Eine industrielle Revolution .....	48
2.9.1	Spezialisierte Rollen .....	49
2.9.2	Bezahlte Mitarbeiter .....	51
2.9.3	Automatisierte Erpresserportale .....	53
2.9.4	Franchising .....	53
2.9.5	Öffentlichkeitsarbeit .....	58
2.9.6	Standardisierte Playbooks und Toolkits .....	64
2.10	Fazit .....	66
2.11	Sie sind dran! .....	66
<b>3</b>	<b>Anatomie eines Angriffs</b> .....	<b>69</b>
3.1	Übersicht .....	70
3.2	Zugang .....	72
3.2.1	Phishing .....	73
3.2.2	Entfernter Login .....	75
3.2.3	Softwareschwachstellen .....	77
3.2.4	Angriffe auf Technologiezulieferer .....	78
3.3	Ausweitung .....	80
3.3.1	Persistenz .....	81
3.3.2	Erkundung .....	82
3.3.3	Ausbreitung .....	82
3.4	Bewertung .....	83

---

3.5	Vorbereitung	84
3.5.1	Antiviren- und Sicherheitssoftware	85
3.5.2	Laufende Prozesse und Anwendungen	85
3.5.3	Logging- und Monitoring-Software	86
3.5.4	Accounts und Zugriffsrechte	87
3.6	Durchführung	88
3.6.1	Ausführen der Ransomware	88
3.6.2	Ausschleusung	89
3.7	Erpressung	93
3.7.1	Passive Mitteilung	94
3.7.2	Aktive Mitteilung	95
3.7.3	Kontakt zu Drittparteien	95
3.7.4	Veröffentlichung	96
3.8	Fazit	96
3.9	Sie sind dran!	96
<b>4</b>	<b>Die Krise beginnt!</b>	<b>99</b>
4.1	Digitale Erpressung ist eine Krise	100
4.2	Erkennung	101
4.3	Wer muss eingebunden werden?	103
4.4	Triage	106
4.4.1	Warum ist Triage wichtig?	107
4.4.2	Beispielhaftes Triage-System	108
4.4.3	Den aktuellen Status einschätzen	108
4.4.4	Wiederherstellungsziele berücksichtigen	109
4.4.5	Die nächsten Schritte bestimmen	110
4.5	Ihre Ressourcen bewerten	111
4.5.1	Finanzen	111
4.5.2	Versicherung	111
4.5.3	Beweissicherung	112
4.5.4	Personal	113
4.5.5	Technische Ressourcen	113
4.5.6	Dokumentation	113
4.6	Eine Strategie für die initiale Reaktion entwickeln	114
4.6.1	Ziele festlegen	114
4.6.2	Einen Aktionsplan entwickeln	115
4.6.3	Verantwortlichkeiten zuweisen	115
4.6.4	Zeit- und Arbeitsaufwand sowie die Kosten schätzen	116

4.7	Kommunizieren Sie . . . . .	116
4.7.1	Response-Team . . . . .	117
4.7.2	Betroffene Parteien . . . . .	118
4.7.3	Die Öffentlichkeit . . . . .	120
4.8	Fazit . . . . .	120
4.9	Sie sind dran! . . . . .	121
<b>5</b>	<b>Eindämmung</b>	<b>123</b>
5.1	Warum Geschwindigkeit zählt. . . . .	124
5.2	Sich Zugang verschaffen . . . . .	125
5.3	Verschlüsselung/Löschung beenden . . . . .	126
5.3.1	Dateizugriffsrechte ändern . . . . .	127
5.3.2	Den Stecker ziehen . . . . .	128
5.3.3	Bösartige Prozesse beenden . . . . .	129
5.4	Persistenzmechanismen deaktivieren . . . . .	129
5.4.1	Monitoring-Prozess . . . . .	130
5.4.2	Terminaufgaben . . . . .	130
5.4.3	Automatischer Start . . . . .	131
5.5	Ausschleusen von Daten beenden . . . . .	131
5.6	Denial-of-Service-Angriffe abwehren . . . . .	132
5.7	Die Hacker aussperren . . . . .	133
5.7.1	Remote-Dienste beenden . . . . .	134
5.7.2	Passwörter lokaler Accounts und von Cloud- Accounts zurücksetzen . . . . .	134
5.7.3	Accounts überprüfen (Audit) . . . . .	136
5.7.4	Multi-Faktor-Authentifizierung . . . . .	136
5.7.5	Perimeter-Kommunikation einschränken . . . . .	136
5.7.6	Minimierung des Drittpartei-Zugangs . . . . .	137
5.7.7	Die Risiken kompromittierter Software minimieren . . .	138
5.8	Suche nach Bedrohungen . . . . .	138
5.8.1	Methodik . . . . .	139
5.8.2	Beweisquellen für das Threat Hunting . . . . .	140
5.8.3	Tools und Techniken . . . . .	140
5.8.4	Mitarbeiter . . . . .	141
5.8.5	Ergebnisse . . . . .	141
5.9	Bestandsaufnahme . . . . .	142
5.10	Fazit . . . . .	143
5.11	Sie sind dran! . . . . .	143

<b>6</b>	<b>Untersuchung</b>	<b>145</b>
6.1	Täterrecherche . . . . .	146
6.1.1	Umsetzungsfähige Sicherheitsinformationen. . . . .	147
6.1.2	Techniken der Identifizierung. . . . .	148
6.1.3	Malware-Stämme. . . . .	152
6.1.4	Taktiken, Techniken und Prozeduren. . . . .	154
6.2	Scoping . . . . .	154
6.2.1	Zu beantwortende Fragen . . . . .	155
6.2.2	Prozess . . . . .	156
6.2.3	Timing und Ergebnisse . . . . .	157
6.2.4	Ergebnisse . . . . .	158
6.3	Einbruch untersuchen oder nicht? . . . . .	158
6.3.1	Rechtliche, regulatorische und vertragliche Pflichten ermitteln . . . . .	159
6.3.2	Entscheidung zur weiterführenden Untersuchung. . . . .	159
6.3.3	Weitere Untersuchung . . . . .	160
6.3.4	Ergebnisse . . . . .	160
6.4	Beweissicherung . . . . .	161
6.4.1	Beweisquellen. . . . .	162
6.4.2	Prioritätenfolge der Volatilität . . . . .	168
6.4.3	Beweissicherung bei Drittparteien . . . . .	169
6.4.4	Gesicherte Beweise speichern . . . . .	169
6.5	Fazit . . . . .	169
6.6	Sie sind dran! . . . . .	170
<b>7</b>	<b>Verhandlung</b>	<b>173</b>
7.1	Es ist ein Geschäft . . . . .	174
7.2	Die Ziele der Verhandlung festlegen. . . . .	175
7.2.1	Budget . . . . .	176
7.2.2	Zeitrahmen . . . . .	177
7.2.3	Informationssicherheit . . . . .	178
7.3	Ergebnisse . . . . .	179
7.3.1	Kauf eines Dekryptors . . . . .	180
7.3.2	Veröffentlichung oder Verkauf von Daten verhindern . .	180
7.4	Formen der Kommunikation . . . . .	182
7.4.1	E-Mail . . . . .	182
7.4.2	Webportal . . . . .	183
7.4.3	Chat-Anwendung. . . . .	184

7.5	Druck aufbauen. . . . .	184
7.6	Ton, Pünktlichkeit und Vertrauen . . . . .	187
	7.6.1 Ton . . . . .	187
	7.6.2 Pünktlichkeit . . . . .	188
	7.6.3 Vertrauen . . . . .	188
7.7	Erstkontakt . . . . .	189
	7.7.1 Erste Nachricht . . . . .	190
	7.7.2 Erste Antwort . . . . .	190
7.8	Informationen teilen . . . . .	191
	7.8.1 Was man nicht teilt . . . . .	192
	7.8.2 Was man teilt . . . . .	193
	7.8.3 Was man für später zurückhält . . . . .	194
7.9	Typische Fehler . . . . .	194
7.10	Lebenszeichen . . . . .	195
	7.10.1 Ziele und Grenzen . . . . .	195
	7.10.2 Bei Zugriffsverweigerung . . . . .	195
	7.10.3 Bei möglichen Enthüllungen . . . . .	197
	7.10.4 Was tun, wenn die Täter den Nachweis ablehnen? . . . . .	197
7.11	Feilschen . . . . .	197
	7.11.1 Preisnachlässe . . . . .	198
	7.11.2 Den Preis festlegen . . . . .	199
	7.11.3 Ein Gegenangebot machen . . . . .	199
	7.11.4 Kompromisse . . . . .	200
7.12	Den Handel abschließen . . . . .	201
	7.12.1 Wie man den Handel abschließt . . . . .	201
	7.12.2 Ihre Meinung ändern. . . . .	202
	7.12.3 Nachdem der Handel abgeschlossen wurde. . . . .	202
7.13	Fazit . . . . .	203
7.14	Sie sind dran! . . . . .	203
<b>8</b>	<b>Zahlung</b>	<b>205</b>
8.1	Zahlen oder nicht zahlen? . . . . .	206
	8.1.1 Ist die Zahlung überhaupt eine Option? . . . . .	206
	8.1.2 Argumente gegen eine Zahlung. . . . .	206
	8.1.3 Argumente für die Zahlung. . . . .	208

8.2	Zahlungsarten . . . . .	209
8.3	Verbotene Zahlungen . . . . .	211
8.3.1	Compliance . . . . .	212
8.3.2	Ausnahmen . . . . .	213
8.3.3	Mildernde Umstände . . . . .	213
8.4	Intermediäre . . . . .	214
8.5	Zeitliche Aspekte . . . . .	215
8.5.1	Verzögerung bei der Überweisung . . . . .	215
8.5.2	Genehmigung durch die Versicherung . . . . .	216
8.5.3	Preisschwankungen bei Kryptowährungen . . . . .	216
8.6	Nach der Zahlung . . . . .	217
8.7	Fazit . . . . .	218
8.8	Sie sind dran! . . . . .	218
<b>9</b>	<b>Wiederherstellung</b>	<b>221</b>
9.1	Backup wichtiger Daten . . . . .	222
9.2	Aufbau der Wiederherstellungsumgebung . . . . .	223
9.2.1	Netzwerksegmente . . . . .	224
9.2.2	Netzwerkgeräte . . . . .	225
9.3	Monitoring und Logging einrichten . . . . .	226
9.3.1	Ziele des Monitorings . . . . .	227
9.3.2	Timing . . . . .	227
9.3.3	Komponenten . . . . .	228
9.3.4	Erkennung und Response . . . . .	229
9.4	Die Wiederherstellung einzelner Computer . . . . .	230
9.5	Reihenfolge der Wiederherstellung . . . . .	232
9.5.1	Domain Controller . . . . .	233
9.5.2	Wichtige Server . . . . .	234
9.5.3	Netzwerkarchitektur . . . . .	235
9.5.4	Arbeitsplatzrechner . . . . .	236
9.6	Daten wiederherstellen . . . . .	238
9.6.1	Datentransfer . . . . .	239
9.6.2	Wiederherstellung aus Backups . . . . .	239
9.6.3	Aktuelle Produktionssysteme . . . . .	241
9.6.4	Daten neu erstellen . . . . .	241

---

9.7	Entschlüsselung . . . . .	241
9.7.1	Übersicht über den Entschlüsselungsprozess . . . . .	242
9.7.2	Arten von Entschlüsselungstools . . . . .	243
9.7.3	Risiken bei Entschlüsselungstools . . . . .	244
9.7.4	Test des Dekryptors . . . . .	245
9.7.5	Entschlüsseln! . . . . .	247
9.7.6	Integrität prüfen . . . . .	248
9.7.7	Auf Malware prüfen . . . . .	248
9.7.8	Daten ins Produktionsnetzwerk transferieren . . . . .	249
9.8	Es ist noch nicht vorbei . . . . .	249
9.9	Anpassung. . . . .	250
9.10	Fazit . . . . .	251
9.11	Sie sind dran!. . . . .	251
<b>10</b>	<b>Prävention</b>	<b>253</b>
10.1	Ein effektives Cybersicherheitsprogramm betreiben . . . . .	254
10.1.1	Wissen, was man zu schützen versucht . . . . .	255
10.1.2	Ihre Pflichten verstehen . . . . .	256
10.1.3	Das Risiko verwalten . . . . .	257
10.1.4	Das Risiko überwachen. . . . .	263
10.2	Zugang verhindern . . . . .	264
10.2.1	Phishing-Abwehr. . . . .	265
10.2.2	Starke Authentifizierung . . . . .	267
10.2.3	Sichere Remote-Access-Lösungen . . . . .	269
10.2.4	Patch-Management . . . . .	270
10.3	Bedrohungen erkennen und blockieren . . . . .	273
10.3.1	Endpunkterkennung und -reaktion . . . . .	274
10.3.2	Netzwerkerkennung und -reaktion . . . . .	275
10.3.3	Suche nach Bedrohungen. . . . .	276
10.3.4	Kontinuierliches Prozess-Monitoring. . . . .	276
10.4	Betriebliche Systemstabilität . . . . .	277
10.4.1	Business-Continuity-Plan. . . . .	278
10.4.2	Nollfallwiederherstellung . . . . .	279
10.4.3	Backups . . . . .	280
10.5	Das Risiko eines Datendiebstahls reduzieren . . . . .	283
10.5.1	Datenreduktion. . . . .	283
10.5.2	Data-Loss-Prevention-Systeme . . . . .	285

10.6	Das Problem der Cybererpressung lösen . . . . .	286
10.6.1	Sichtbarkeit erzeugen . . . . .	286
10.6.2	Erkennung und Monitoring fördern . . . . .	287
10.6.3	Proaktive Lösungen fördern . . . . .	288
10.6.4	Die Macht der Täter reduzieren . . . . .	288
10.6.5	Das Risiko für die Täter erhöhen . . . . .	289
10.6.6	Den Profit der Täter verringern . . . . .	290
10.7	Fazit . . . . .	291
10.8	Sie sind dran! . . . . .	292
<b>Nachwort</b>		<b>295</b>
<b>Checkliste A</b>		<b>297</b>
	Response auf Cybererpressung . . . . .	297
	Die Krise beginnt . . . . .	297
	Eindämmung . . . . .	298
	Untersuchung . . . . .	299
	Verhandlungen . . . . .	300
	Zahlung . . . . .	301
	Wiederherstellung . . . . .	301
<b>Checkliste B</b>		<b>303</b>
	Im Vorfeld zu entwickelnde Ressourcen . . . . .	303
	Response-Pläne . . . . .	303
	Krisenkommunikationspläne . . . . .	304
	Weitere Vorgehensweisen . . . . .	304
	Kontaktinformationen . . . . .	304
	Während der Response zu nutzende Vorlagen . . . . .	305
	Die Response unterstützende Technik . . . . .	305
	Referenzmaterial . . . . .	306
<b>Checkliste C</b>		<b>307</b>
	Die Response planen . . . . .	307

<b>Checkliste D</b>	<b>309</b>
Ein effektives Cybersicherheitsprogramm betreiben . . . . .	309
Wissen, was Sie zu schützen versuchen . . . . .	309
Ihre Pflichten verstehen. . . . .	309
Das Risiko steuern . . . . .	310
Das Risiko überwachen . . . . .	311
<b>Index</b>	<b>315</b>