1 Einleitung 1
1.1 Lesehinweise 2
1.2 Fokus Mittelstand 3
1.3 Fokus Ransomware 3
1.4 Dankeschön 3

2 Kurzeinstieg für Manager 5

Teil I Wie funktioniert Ransomware?

3 Evolution der Bedrohungslage 17
3.1 Was ist eine Bedrohung? 18
3.2 Angriffsvektoren 18
3.3 Veränderte Bedrohungslage 19

4 Die Täter und ihre Motivation 21
4.1 Geschichte 21
4.1.1 Ab 2012: Angriffe gegen Privat-PCs 22
4.1.2 Ab 2015: Professionalisierung 23
4.1.3 2017: Spezialfall WannaCry 26
4.1.4 Bis heute: Cashcow der Organisierten Kriminalität 30
4.2 Verfolgungsdruck 32
4.2.1 Ermittlungserfolge 33
4.2.2 Abschreckung 34
4.2.3 Schwierigkeiten in der Strafverfolgung 35
4.3 Organisation 36
4.3.1 Zusammensetzung des Teams 37
4.3.2 Funktionalität eines Ransomware-Toolkits 38
4.3.3 Regeln für Affiliates 41
4.3.4 Aufnahmekriterien 42
4.3.5 Vorteile eines RaaS-Dienstleisters 43
4.3.6 Schwankender Organisationsgrad in der Szene 44

Bibliografische Informationen
https://d-nb.info/1285812565

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4.4 Erpressungsmethodik ... 45
4.4.1 Verschlüsselung ... 47
4.4.2 Datenveröffentlichung ... 48
4.4.3 Erneuter Angriff ... 51
4.4.4 Erpressungssummen ... 52
4.5 Auswahl der Opfer ... 56
4.5.1 Ransomware-Angriffe sind ungezielt ... 56
4.5.2 Ransomware-Angriffe sind vermeidbar ... 57
4.6 Täterprofil ... 59
4.6.1 Herkunft der Täter ... 59
4.6.2 Motivation und innere Rechtfertigung ... 60
4.6.3 Können und Ausbildung ... 60

5 Taktik, Tools und Vorgehen der Angreifer ... 61
5.1 Phasen des Angriffs ... 63
5.2 Initial Compromise ... 64
5.2.1 Angriffe auf Systeme im Internet ... 65
5.2.2 Phishing ... 68
5.2.3 Attachment-Malware ... 70
5.3 Remote Access Trojaner (RAT) ... 76
5.3.1 C2 über Applikationsprotokolle ... 78
5.3.2 Consumer Tools ... 79
5.3.3 Post-Exploitation Tooling ... 80
5.3.4 Spezialfall: Living off the Land (LoL) ... 81
5.4 Local Privilege Escalation ... 81
5.4.1 Privilege Escalation von Medium-Integritätslevel ... 82
5.4.2 User-Account-Control-Bypass (UAC-Bypass) ... 84
5.4.3 Escalation zu System Integrity Level ... 84
5.5 Lateral Movement und Global Privilege Escalation ... 85
5.5.1 Internal Reconnaissance ... 85
5.5.2 Local Admin Accounts ... 87
5.5.3 Low-Tech Credential Harvesting ... 87
5.5.4 Angriffe auf NTLM-Authentifizierung ... 88
5.5.5 Angriffe auf Kerberos ... 91
5.5.6 Schwachstellen zur Global Privilege Escalation ... 95
5.6 Data Exfiltration ... 97
5.6.1 Exfiltration mit Standard-Tools ... 97
5.6.2 Spezialtool: StealBIT ... 98
5.6.3 Spezialtool: ExMatter ... 98
5.6.4 Erkennung von Exfiltration ... 98
5.7 Attacking the Backup ... 99
5.7.1 Lokale Backups ... 99

5.7.2 Zentrale Backups ... 100
5.7.3 Erkennung ... 100
5.8 Encryption ... 100
5.8.1 Verteilung und Ausführung der Verschlüsselung ... 100
5.8.2 Vorbereitung der Verschlüsselung ... 102
5.8.3 Datenverschlüsselung ... 102
5.8.4 Erkennung ... 104
5.9 Attack Closing ... 104

Teil II Es ist passiert!

6 Erst- und Sofortmaßnahmen ... 109
6.1 Indizien Ransomwarebefall ... 111
6.2 Sofortmaßnahmen bei Ransomwarebefall ... 114
6.2.1 Isolation des Netzwerks ... 114
6.2.2 Außenstellen informieren/sichern ... 114
6.2.3 Backup in Sicherheit bringen ... 115
6.2.4 Stoppen der Verschlüsselung ... 115
6.2.5 Externe Zugänge sichern ... 116
6.3 Team zusammenstellen ... 117
6.4 Erster Plan für den Kriseneinsatz ... 118

7 Open Source Intelligence (OSINT) ... 121
7.1 Identifikation der Angreifer ... 122
7.2 Dossier zum Angreifer zusammenstellen ... 123

8 Schadensausmaß verstehen ... 127
8.1 Ausmaß der Verschlüsselung ... 127
8.2 Stand des Backups ... 128
8.3 Auswirkungen auf die Unternehmensprozesse ... 128
8.4 Ausmaß der Datenausleitung ... 129

9 Organisation der Krisenbewältigung ... 131
9.1 Zwei starke, fokussierte Krisenorganisationen ... 132
9.1.1 Crisis Management Team (CMT) ... 132
9.1.2 Cyber Security Incident Response Team (CSIRT) ... 134
9.2 Das erste CMT-Meeting ... 135
9.3 Die Arbeit im CSIRT ... 136
9.4 Dokumentation der Arbeit ... 137
9.4.1 Beispiel anonymisierte Fallbeschreibung ... 137
9.4.2 Beispielhaftes CMT-Protokoll ... 138
9.5 Arbeitsteilung in größeren Unternehmen ... 138
9.6 Beenden des Krisenmodus ... 142

10 Aufbau Notbetrieb 143
10.1 Ziel des Notbetriebs definieren 144
10.2 Netzwerksegmentierung 145
10.3 Liste wichtigster IT-Systeme und Applikationen 146
10.4 Notbetrieb implementieren 146
10.5 Infrastruktur im Notbetrieb 147
10.6 Beweissicherung im Notbetrieb 149
10.7 Notbetrieb durchführen 149
10.8 Beispielhafter Ablauf 149

11 Täterkommunikation 151
11.1 Rollentrennung Entscheider – Verhandler 152
11.2 Verhandlungstechniken 152
11.3 Eintritt in die Kommunikation 153
11.4 Zeit gewinnen 156
11.5 Karten auf den Tisch 158
11.6 Lösegeldverhandlung 159

12 Erpressungsgeldzahlung 167
12.1 Rechtliche Aspekte 168
12.1.1 Verstöße gegen Sanktionsrecht 168
12.1.2 Unterstützung einer kriminellen Vereinigung 169
12.1.3 Strafbarkeit wegen Geldwäsche 170
12.1.4 Bankenaufsichtsrechtliche Erwägungen 170
12.2 Zahlungsabwicklung 171

13 Krisenkommunikation 175
13.1 One Voice Policy 176
13.2 Kommunikationsinhalte 176
13.3 Zeitpunkt und Verteilung 179
13.4 Weiterführende Informationen 179
13.5 Überraschende und aggressive Fragen 180
13.6 Runtermanagen 181
13.7 Beispiele 181
13.7.1 Kundeninformation Medienunternehmen 182
13.7.2 Presseinformation Produktionsunternehmen 183
13.7.3 Mitarbeiterinformation Mischkonzern 184

14 Compliance Stakeholdermanagement 185
14.1 Strafverfolgungsbehörden 186
14.2 Datenschutzaufsichtsbehörde 187
14.3 Versicherung 189

15 Forensik ... 191
15.1 Stakeholder in der Forensik ... 192
15.1.1 CSIRT ... 192
15.1.2 Verhandler ... 192
15.1.3 Cyberversicherung ... 193
15.1.4 Behörden und Strafverfolgung ... 193
15.1.5 Community ... 194
15.2 Dokumentation ... 194
15.2.1 Quellendokumentation ... 195
15.2.2 Timeline ... 195
15.2.3 Indicators of Compromise ... 196
15.2.4 Statusbericht ... 198
15.2.5 Fallübersicht im Verflechtungsdiagramm ... 199
15.3 Sicherung der Beweise ... 199
15.3.1 Beweissicherung vs. Notbetrieb ... 200
15.3.2 Bewährte Methoden zur Beweissicherung ... 201
15.4 Cloud-Forensik ... 202
15.5 Live-Forensik und Threat Hunting ... 203
15.6 Ransomware-Forensik ... 204
15.6.1 Artefakte auf Windows-Systemen ... 204
15.6.2 Artefakte auf DCs ... 205
15.6.3 Firewall-Logs ... 205
15.6.4 Backupsystem ... 206
15.7 Forensik Werkzeuge ... 206

16 Wiederherstellung ... 207
16.1 Wiederaufbaustrategien ... 207
16.2 Wiederaufbau planen ... 208
16.3 Wiederherstellungsstrategie „Säubern“ ... 210
16.3.1 Forensik durchführen ... 211
16.3.2 Netzwerk vorbereiten ... 211
16.3.3 Infrastrukturkonfiguration säubern ... 211
16.3.4 Server und Clients säubern ... 213
16.3.5 Sichtbarkeit erhöhen ... 215
16.3.6 Internetzugang reglementieren ... 217
16.3.7 Restrisiko akzeptieren ... 218
16.4 Wiederherstellungsstrategie „Neuaufbau“ ... 218
16.4.1 Ressourcen sichern ... 219
16.4.2 Planung Zukunft ... 219
16.4.3 Basisinfrastruktur implementieren ... 220
16.4.4 Sicherheitsinfrastruktur aufbauen ... 221
16.4.5 Dienste migrieren ... 222

16.4.6 Client-PCs neu aufsetzen ... 225
16.5 IT-Wiederherstellungsstrategie „Entschlüsseln" ... 226
16.6 Backup wieder einrichten ... 228
16.7 Zusammenfassung ... 228

17 Schäden und Schadenshöhe ... 231
17.1 Eigenschäden des Unternehmens ... 232
17.1.1 Betriebsunterbrechungsschaden ... 232
17.1.2 IT-Forensik ... 233
17.1.3 Wiederherstellungskosten ... 233
17.1.4 Systemverbesserungen ... 234
17.1.5 Krisenmanagement ... 234
17.1.6 Krisenkommunikation und Reputationsschaden ... 235
17.1.7 Rechtliche Beratung und datenschutzrechtliche Notifizierung ... 235
17.2 Haftpflichtschäden ... 236
17.2.1 Haftung des Unternehmens nach DSGVO ... 236
17.2.2 Datenschutzrechtliche Bußgelder ... 236
17.2.3 Vertragliche Haftung gegenüber Geschäftspartnern ... 237
17.2.4 Haftung von Geschäftsleitern für Cyberangriffe ... 237

Teil III Ich will nicht, dass es passiert!

18 Präventives Krisenmanagement ... 241
18.1 Krisenprävention ... 242
18.2 Krisenhandbuch erstellen ... 243
18.3 Krisenstabstraining ... 249

19 Moderne Security-Strategien ... 251
19.1 Defend the Perimeter ... 251
19.2 Assume Breach ... 252
19.3 Defense in Depth ... 253

20 Alarmstufen im Information Security Management System (ISMS) ... 255
20.1 Reaktive Sicherheit als Aufgabe der CISO-Organisation ... 255
20.2 Vorbereitungen für das Alarmstufenmanagement ... 260
20.3 Tatorthygiene für Administratoren ... 261
20.4 Alarmstufe Gelb: 100 % Wachsamkeit ... 262
20.5 Alarmstufe Orange: Schilde hoch, Waffen bereit machen ... 264

21 Technische Abwehr von Angriffen ... 267
21.1 Phishing-Schutz ... 268
21.2 Client Hardening ... 269
21.3 Zugänge von außen kontrollieren ... 270

21.4 Offline-Backup 270
21.5 Domäne schützen 271
21.6 Erkennung von Angriffen im internen Netz 272
21.7 Patch Management 273
21.8 Netzwerksegmentierung 273
21.9 Virtualisierungsinfrastruktur 274
21.10 Cloud-Umgebungen 275
21.11 Vorbereitung auf den Ernstfall 275
21.12 Nicht verhandelbar 276

22 Cyber-Security-Schnelltests 277
22.1 Phishing 278
22.2 Passwortangriff 278
22.3 Scan nach Zugängen 279
22.4 Schadsoftware 279
22.5 Backups löschen 280
22.6 Wiederherstellung 281
22.7 Neue Clients 281
22.8 Bewertung 282

23 Abschluss einer Cyberversicherung 285
23.1 Für welche Unternehmen ist eine Cyberversicherung sinnvoll? 285
23.2 Welche Schäden deckt eine Cyberversicherung ab? 287
23.2.1 Baustein Dienstleistung 287
23.2.2 Baustein Eigenschaden 288
23.2.3 Baustein Haftpflichtschäden 288
23.3 Der Teufel steckt im Detail 289
23.3.1 Obliegenheiten und Gefahrenerhöhungen 289
23.3.2 Cyber-Werkstattbindung 290
23.3.3 Vorbereitung auf den Krisenfall 290
23.3.4 Schadensregulierung kann dauern 290
23.3.5 Erfahrene Makler helfen 291

Teil IV Was wird uns die Zukunft bringen?

24 Die Zukunft der Ransomware 295
24.1 Professionalisierung der Erpressung 295
24.2 Cloud und IT-Supply Chain als neues Ziel 295
24.3 Ransomware going Cyber-Physical 296
24.4 Ransomware im geopolitischen Kontext 296
24.5 Einsatz von Zero Days 297

25 Anhang 299
25.1 BSI Informationen zu Ransomware 299
25.2 Beispiele für OSINT-Analysen 299
25.2.1 OSINT für einen frühen Black-Basta-Fall 300
25.2.2 OSINT für einen HIVE-Fall 300
25.2.3 OSINT für einen ROYAL-Fall 303
25.3 Log-Einstellungen für Windows-Systeme 304
25.4 Sysmon-Konfiguration 308
25.5 Whitelist für Dateiendungen 308
25.6 BIOS-Einstellungen 308
25.6.1 Generelle Konfiguration: 309
25.6.2 Virtualisierung 309
25.6.3 Intel Management Engine/Computrace (Absolute Pers.) 310
25.6.4 Bootkonfiguration 310
25.6.5 TPM und Passwort 310
25.7 Suchmaschinen für Sicherheitsexperten: 311
25.8 Literatur Verhandlungstechniken 312
25.9 Forensik Tools 312